المركز الديمقراطي العربي؛ برلين- ألمانيا

الجريمة المعلوماتية وأثرها على التنمية الاقتصادية



اشراف وتنسيق
د. مجدوب نوال
رئيس اللجنة العلمية
د. طالب محمد كريم

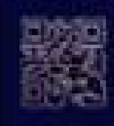
كتاب جماعي

الجزء:01

رقم التسجيل: VR.3373.6395.B

المركز الديمقراطي العربي
الجريمة المعلوماتية وأثرها على التنمية الاقتصادية





الجريمة المعلوماتية وأثرها على التنمية الاقتصادية

الجزء:01

إشراف و تنسيق:

د. مجدوب نوال



الناشر

المركز الديمقراطي العربي

للدراسات الاستراتيجية والسياسية والاقتصادية

ألمانيا/برلين

Democratic Arabic Center

Berlin / Germany

المركز الديمقراطي العربي

للدراسات الاستراتيجية والسياسية والاقتصادية ألمانيا/برلين

Berlin10315 Gensingerstr :112

Tel :0049-code Germany

54884375-030

91499898-030

86450098-030

البريد الإلكتروني

book@democraticac.de



رئيس المركز الديمقراطي العربي: أ.عمار شرعان

اسم الكتاب: الجريمة المعلوماتية و أثرها على التنمية الاقتصادية

الجزء: 01

تأليف: مجموعة من الباحثين

إشراف والتنسيق: د. مجدوب نوال

رئيس اللجنة العلمية للكتاب: د. طالب محمد كريم

ضبط وتدقيق: د. سالم بن لباد

التصميم والإخراج: د. بدر الدين شعباني

رقم تسجيل الكتاب: VR.3373.6395.B

عدد الصفحات:

الطبعة الأولى

جويلية 2020 م

المحتويات

اللجنة العلمية للكتّاب :

لجنة تحكيم الكتاب

تأليف مجموعة من الباحثين

د. حمادة خير جامعة العراق	د .عائشة الجميل جامعة الأسيوط	د.باعزيز أحمد المركز الجامعي مغنية
د. الأحسن محمد المركز الجامعي مغنية	د. تلعيش خالد جامعة خميس مليانة	د. حماس عمر المركز الجامعي مغنية
د. معاشو لخضر جامعة بشار	د. سويلم فضيلة جامعة سعيدة	د.دربال سهام المركز الجامعي مغنية



مقدمة

تأليف مجموعة من الباحثين

مقدمة الكتاب

لا يمكن إنكار المزايا التي قدمتها تكنولوجيا الإعلام و الاتصال في كافة مجالات الحياة ، إذ وبالقدر الذي ساهمت المعلوماتية في النهوض و التقدم و الرقي ، بقدر ما ساهمت في بروز نوع مستحدث من الإجرام و هو الإجرام المعلوماتي ، و الذي أخذ عدة تسميات و من ذلك الجريمة الإلكترونية ، جرائم الحاسوب ، جرائم تكنولوجيا الإعلام و الاتصال ، الجريمة الرقمية ،الجريمة السيبرانية ، جريمة الانترنيت، الجريمة الرقمية .

و بالتالي فالجريمة المعلوماتية تشكل نمط إجرامي مستحدث فرض نفسه على الواقع ، و تعرف على أنها كل سلوك إيجابي أو سلبي تقدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة من أجل تنفيذ فعل إجرامي.

و تأخذ الجريمة المعلوماتية عدة صور فقد يكون الغرض من ارتكابها التعدي على العرض والشرف، أو الأموال، أو المساس بنزاهة التجارة و أخلاقيات التسويق، أو الاعتداء على حقوق الملكية الفكرية ، بل و أكثر من كذلك فقد استهدفت الجريمة المعلوماتية قطاع الخدمات.

وانطلاقا من مضار الجريمة المعلوماتية فإن هذه الأخيرة تكيف من قبيل الجرائم الاقتصادية، باعتبار أنها تستنزف اقتصاديات الدول، و يترتب عنها نتائج تنعكس سلبا على التنمية الاقتصادية، مما حتم معه ضرورة تضافر الجهود الوطنية و الدولية.

ونظرا لذاتية الجريمة المعلوماتية فقد أخذ إجراءات المتابعة بدورها خصوصية، سواء من حيث التفتيش أو التحري، أو حتى العقوبة ولاسيما في ظل غموض الدليل الرقمي .

ولأنه يعتري تنظيم الجريمة المعلوماتية في التشريع الجزائري، و التشريعات المقارنة عدة إشكالات، كان لزاما الخوض في هذا الموضوع بشتى جوانبه و تفريعاته، من طرف ثلة من الباحثين والباحثات، اللذين أسهموا بجهودهم الجادة في إخراج هذا العمل المتواضع إلى النور.



المحور الأول

الإطار العام للجريمة المعلوماتية

تأليف مجموعة من الباحثين

الإطار المفاهيمي للجريمة المعلوماتية

The conceptual framework for information crime

بن سعيد **خالد** طالب دكتوراه
د. **عثماني عبد الرحمان** أستاذ محاضر أ
كلية الحقوق والعلوم السياسية
جامعة مولاي الطاهر بسعيدة

مقدمة

كان للتقدم العلمي الهائل في مجال وسائل التكنولوجيا والاتصال دور في خلق ثورة في المعلوماتية، وما أفرزته من أجهزة المراقبة والتنصت و التسجيل والتقاط الصور وسهولة التواصل والحصول على المعلومة ،فأصبح من اليسير غزو خصوصية الإنسان والمؤسسات سواء داخل الوطن او خارجه من خلال هذه الوسائل الحديثة المتطورة .

حيث ان التطور التكنولوجي الحديث ،أصبح يشكل تهديدا خطيرا للعديد من عناصر الحياة الخاصة كالمكالمات الهاتفية والمراسلات والمعلومات والبيانات الشخصية ،وكذا في تسهيل الجرائم وتوسعها وتنوعها و التي قد تمس ، الأموال ، الأشخاص و ممتلكاتهم كالسحب الالكتروني والقرصنة ...

وتحدد أهمية الموضوع في إعطاء تعريفات خاصة بظاهرة جديدة تسمي الجريمة المعلوماتية، من خلال ضبط صفة الجاني ونوع الوسائل المستخدمة وكذا اتساع نطاقها لتشمل جميع المجالات، وبالتالي ضبط نوع الجريمة التي تكتسي طابع خاصا يقوم على استخدام الانترنيت والتكنولوجيا المتطورة في ارتكابها بسهولة سواء داخل الوطن او خارجه مع صعوبة اثباتها، وبالتالي عدم القدرة للوصول للجاني .وهذا ما يؤدي الى ضرورة بيان المفاهيم الخاصة بالجريمة المعلوماتية.

فالهدف من هذه الدراسة هو تسليط الضوء على جريمة حديثة تسمى "الجريمة المعلوماتية " وتحليل مفهومها ، فهي تعتمد على مهارات وفنيات في ارتكابها مع سهولة مسح الدليل ، وهي عادة ما ترتكب بواسطة اجهزة متطورة عن طريق الكومبيوتر (الحاسب الالي) او الهواتف الذكية بواسطة الانترنيت وغيرها من الوسائل الحديثة .وقد ترتكب بواسطة فرد او عدة افراد في مناطق قد تكون عابرة للدول فقد يكون الجاني في بلد والفاعل في بلد أخر .ومنه كان لزاما على المشرع

الجزائري كمرحلة اولى تحديد وضبط مفهوم الجريمة المعلوماتية بسن قوانين تنظمها وتحدد جوانبها وكذا العقوبات المستوجبة .

وعليه نطرح الاشكالية التالية :ما مدى تجسيد مفهوم الجريمة المعلوماتية من قبل المشرع الجزائري ؟

وقبل الإجابة على هذه الإشكالية سوف يتم التعرض لبعض المفاهيم (مدخل تمهيدي مفاهيمي) بالإضافة إلى عناصر الجريمة المعلوماتية (المحور الأول)، ناهيك عن سمات و خصوصية الجريمة المعلوماتية لتميزها عن الجريمة التقليدية (المحور الثاني)

مدخل مفاهيمي للدراسة :

تتجلى المفاهيم التي تدور حولها الدراسة في مايلي :

أولا : تعريف المعلومات هناك تعريفين للمعلومات لغوي واصطلاحي

1- **التعرف اللغوي للمعلومات :** يرجع اصل ومدلول كلمة المعلومات الى اللغة اللاتينية information ومفادها شرح او توضيح شيء ما ،وهي نفسها الكلمة بالإنجليزية على اعتبارها نشاطا اتصاليا ، اي يتضمن عملية مشاركة في المعنى من خلال نقل معلومات معينة من طرف لأخر وذلك بإعطاء الجمهور العديد من المعلومات عن الأحداث و الظواهر والمشكلات بطريقة صحيحة وموضوعية[1].

2- **التعريف الاصطلاحي للمعلومات :** المعلومات هنا هي التعبير الحقيقي او الملموس للعمليات المعرفية التي تحدث في العقل الإنساني ،وبالتالي فهي نتاج العملية المعرفية التي تظهر في شكل كيان مادي [2].

وهناك من يعرف المعلومات على أنها : "مجموعة من الرموز أو الحقائق أو المفاهيم او التعليمات التي تصلح لان تكون محلا للتبادل والاتصال أو التفسير أو التأويل أو المعالجة ،التي تتم بواسطة الأفراد أو الأنظمة الالكترونية" [3] . وحتى تتمتع المعلومات بالحماية يجب أن تتوافر فيها مجموعة من الشروط والتي من بينها :

---

[1]-منال هلال المزاهرة، تكنولوجيا الاتصال والمعلومات ، دار المسيرة للنشر و التوزيع ، الطبعة الاولى 2014، عمان ، ص 27-28 .

[2]- منال هلال المزاهرة ، مرجع سابق ،ص 28 .

[3]-طارق ابراهيم الدسوقي عطية ، الامن المعلوماتي (النظام القانوني للحماية المعلوماتية)،دار الجامعة الجديدة للنشر ،طبعة 2009 ، ص 38.

ا-ان تتسم المعلومة بالتحديد والابتكار : اي يمكن حصرها في دائرة معرفية عن طريق رموز أو بيانات او إشكال وان تنصب على شيء محدد .وان تكون المعلومة مبتكرة وغير عامة .

ب-السرية والاستئثار في المعلومة :أي حماية المعلومة التي تتسم بالسرية المعلومة الخاصة بأحد الاكتشافات العلمية او المعلومات الأمنية السرية ،عكس المعلومة العامة التي يطلع عليها الجميع كالواردة في نشرة الأخبار ، كما يعد الاستئثار خاصية مهمة لاستئثار شخص بالمعلومة او عدة أشخاص للتصرف فيها ، وفي هذه الحالة يكون الاستئثار لمؤلف المعلومة[1].

ثانيا : مفهــــــوم المعلوماتية

ان استعمال هذا المصطلح يعود للاتحاد السوفياتي سابقا لسنة1967 حيث تم صياغته بالروسية informatik ،وهو ما يعني نشر المعلومات الالكترونية عبر الشبكات [2].

كما عرفت الاكاديمية الفرنسية في جلستها المنعقدة بتاريخ 6 افريل 1967 المعلوماتية على أنها:"علم التعامل العقلاني ، وعلى الاخص بواسطة الآلات الاوتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الانسانية وعمادا للاتصالات في ميادين التقنية والاقتصاد والاجتماع " .ويرى البعض بان المعلوماتية هي "علم المعالجة المنطقية والآلية للمعلومات"[3].

ثالثا :مسميات الجريمة المعلوماتية

تتعدد الاسماء التي تطلق على مصطلح الجريمة المعلوماتية ، وهذا ناتج عن التطورات الحديثة في مجال الحاسب والانترنيت والتي من بينها :جرائم الحاسوب والانترنيت ،جرائم التقنية العالية ، الجريمة الالكترونية ، الجريمة السيبيرانية ...[4].

المحور الأول : تعريف الجريمة المعلوماتية

كان للثورة المعلوماتية دور كبير في خلق وسائل التواصل الحديثة والمتطورة كشبكات الانترنيت والحاسوب والهواتف الذكية وهو ما أدى الى ظهور الجريمة المعلوماتية، حيث يعتمد مرتكبها على وسائل تقنية ويكون ذا علم بالنظم المعلوماتية والتقنية ، أدت الى تسهيل الارتباط بين

---

[1]- طارق ابراهيم الدسوقي عطية ، مرجع سابق ، ص40-41 .

[2]-منال هلال المزاهرة ،مرجع سابق ، ص 37.

[3]-سامي على حامد عياد ،الجريمة المعلوماتية واجرام الانترنيت ،دار الفكر الجامعي ، طبعة 2008 ،ص 35-36.

[4]-حسنين شفيق ، الاعلام الجديد والجرائم الالكترونية ، التسريبات ، التجسس ، الارهاب الالكتروني ، دار فكر وفن للطباعة والنشر والتوزيع ،2014 ،ص 17 .

المؤسسات والافراد من داخل الوطن وخارجه ، وعليه سيتم التطرق في المطلب الأول إلى عناصر المعلوماتية المتمثلة في الحاسب والانترنيت ثم لتعريف الجريمة المعلوماتية من الناحية القانونية في مطلب ثان ثم لمفهومها من الناحية الفقهية في المطلب الثالث ، وفي المطلب الرابع سيتم التطرق للمفهوم الدولي للجريمة المعلوماتية

المطلب الاول : عناصر المعلوماتية

ان تطور المجتمعات ادى بالضرورة لتطور وسائل الاتصال بظهور التكنولوجيا الحديثة ، كاستعمال الحاسوب والهواتف الذكية والانترنيت وكذا سهولة ربط الجناة مع بعضهم من خلال وسائل التواصل عبر شبكات الانترنيت ،وعليه سوف يتم تناول عناصر المعلوماتية في هذا المطلب من خلال فرعين :(الفرع الاول) يتناول الحاسوب اما الثاني فيتناول الانترنت .

الفرع الاول : الحاسوب

يعد من أهم الأدوات الداخلة في ارتكاب الجرائم المعلوماتية، فالحاسب الالي لغة يعني بالإنجليزية computer وهي كلمة مشتقة من الفعل comput بمعنى يحسب او يحصي ، ويقابلها باللغة الفرنسية كلمة ordinateur وتعني ناظمة الية [1]

فالحاسب عبارة عن جهاز الكتروني يستطيع ان يقوم بأداء العمليات الحسابية والمنطقية بسرعة كبيرة مع قدرته على التعامل مع الكم الهائل في معالجة البيانات او استرجاعها او تخزينها .

كما يعرف بانه جهاز الكتروني يستطيع ترجمة اوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات ادخال البيانات data input او اخراج معلومات information output واجراء عمليات حسابية ومنطقية وهو يقوم بالكتابة على اجهزة الاخراج output devices او تخزين البيانات التي يتم ادخالها بواسطة مشغل الحاسب operator عن طريق وحدات الادخال [2] .

الفرع الثاني: الانترنت

عرف المشرع الجزائري من خلال المادة 3 من المرسوم 98-257 المتعلق بشروط اقامة خدمات الانترنت " بأنه اي مكان يحتوي موزعا او عدة موزعات للمعطيات الضرورية لتقديم خدمات الانترنت "

---

[1]- طارق ابراهيم الدسوقى عطية ، مرجع سابق ، ص 73 .

[2]- عبد العال الديربي ، محمد صادق اسماعيل ، الجرائم الالكترونية (دراسة قانونية قضائية مقارنة مع احث التشريعات العربية في مجال مكافحة الجرائم المعلوماتية والانترنت) ، الطبعة الاولى 2012 ، المركز القومي للإصدارات القانونية ، القاهرة ، ص 15-16 .

وامام هذا التطور الهائل في شبكة الانترنت الذي سمح بالربط الدولي من خلال استقبال المعلومات وتخزينها وتوزيعها ، تم سن العديد من التشريعات بغية وضع حد بين الحرية في استعمال شبكة الانترنت وبين المسؤولية الناتجة عن استعمالها [1] .

فالإنترنت هو جزء من ثورة الاتصالات ومنهم من يرى بانها شبكة طرق المواصلات السريعة وتعني لغويا (ترابط بين الشبكات) لأنها تتكون من عدد كبير من شبكات الحاسب المترابطة في انحاء العالم والتي ينظمها بروتوكول يسمى (بروتوكول تراسل الانترنت TCP\IP) [2] .

كما ان كل شبكة انترنيت تدار بالطرية التي يراها اعضاؤها او مجتمعها بوضع مجموعة من المبادئ والضوابط التي تسير الانترنيت بالتحكم في اتجاهها ، والاحاطة بهذه المعلومات امر ضروري لمن يريد ان يدخل في الشبكة ويستفيد من خدماتها ، مع العلم ان خدمات الانترنيت تتحكم فيها الدولة [3].

ومن خلال هذين العنصرين (الحاسب الالي والانترنت) ظهرت بوادر الجريمة المعلوماتية ، حيث تعرف هذه الجرائم بانها :" ذلك النوع من الجرائم التي تتطلب الماما خاصا بتقنية الحاسب الالي ونظم المعلومات لارتكابها او التحقيق فيها ومقاضاة فاعلها ") [4].

المطلب الثاني : التعريف القانوني للجريمة المعلوماتية

لقد تعددت التعاريف الخاصة بالجريمة المعلوماتية وتختلف من تشريع لأخر ، حيث استحدث المشرع الجزائري نصوصا تخص الاعتداء على الشبكة المعلوماتية بموجب القانون رقم 04-15 مؤرخ في 2004/11/10 المتضمن تعديل قانون العقوبات[5] ، حيث تناول الاعتداءات الماسة بالأنظمة المعلوماتية والتي نوجزها فيما يلي [6]:

- جريمة التوصل او الدخول غير المصرح به : نصت عليها المادة 394 مكرر من قانون العقوبات.

---

[1]- زيجة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى ، الجزائر طبعة 2011 ، ص 26 وما بعدها .

[2]- سامي علي حامد عياد ، مرجع سابق ، ص 67 .

[3]-منال هلال المزاهرة ، مرجع سابق ، ص 309 .

[4]- سامي علي حامد عياد ، مرجع سابق ،ص 71 .

[5]- قانون رقم 04-15 المؤرخ في 10نوفمبر 2004 ، المعدل والمتمم للأمر رقم 66-156 مؤرخ في 08 جوان 1966 المتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية، العدد 71مؤرخة في 2004/11/10 .

[6]-المواد من 394 مكرر الى 394 مكرر2 من قانون العقوبات رقم 99-165 المعدل والمتمم ،مرجع سابق .

- جريمة التزوير المعلوماتي : نصت عليها المادة 394 مكررا1 من قانون العقوبات .
- جريمة الاستيلاء على المعطيات العقوبات .-جريمة اتلاف وتدمير المعطيات -جريمة الاحتيال المعلوماتي
- انشطة الانترنت المجسدة لجرائم المحتوى الضار والتصرف الغير القانوني من ذلك ما نصت عليه المادة 394 مكرر2 /2 على تجريم افعال الحيازة النشر...

وقد سبقه المشرع الفرنسي في ذلك بكثير من خلال اصداره للقانون رقم 88-19 المؤرخ في 05-01-1988 المتعلق بالغش المعلوماتي والذي يسمى بقانون قودفرا godfrain[1] والذي ميز بين الاعتداء على برامج ومعلومات الحاسب الالي وبين الاعتداء على ادواته ومعداته ،فنص على جرائم الاعتداء على برامج ومعلومات الحساب الرقمي الالي بجريمتين :

-جريمة التوصيل بطريق التحايل لنظام المعالجة الالية للبيانات
-جريمة اتلاف برامج ومعلومات الحاسب الالي الرقمي .

اما بخصوص جرائم الاعتداء على ادواته ومعداته فحصرها فيما يلي :

-جريمة اتلاف الادوات الحاسب الالي الرقمي
-جريمة الاستخدام غير المستحق لأدوات والات الحاسب الرقمي الالي [2]

كما قام المشرع الجزائري بضبط المصطلحات الخاصة بالجريمة المعلوماتية من خلال المادة 2 من القانون 09-04 [3] المتضمن القواعد المطبقة على الجرائم المتصلة بجرائم تكنولوجيات الاعلام والاتصال ومكافحتها بتحديد تعريف كل من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، منظومة معلوماتية ،معطيات معلوماتية ،مقدمو الخدمات ،المعطيات المتعلقة بحركة السير واخيرا الاتصالات الالكترونية .وعرفها كالاتي :

---

[1]-رابح وهيبة الجريمة المعلوماتية في الاجراء التشريعي الجزائي ،مجلة الباحث للدراسات الاكاديمية ،العدد الرابع، ديسمبر 2014 ، ص 322

[2]- سميرة معاشي ،الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)،مجلة المفكر ، العدد 17 ،جوان 2018 ، ص 407 .

[3]-القانون رقم 09-04 المؤرخ في 05 غشت 2009 المتضمن القواعد المطبقة على الجرائم المتصلة بجرائم تكنولوجيات الاعلام والاتصال ومكافحتها الجريدة الرسمية للجمهورية الجزائرية ، العدد 47 بتاريخ 16 غشت 2009 .

ا-الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال :جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات واي جريمة اخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية .

ب-منظومة معلوماتية : اي نظام منفصل او مجموعة من الانظمة المتصلة ببعضها البعض او المرتبطة ، يقوم واحد منها او اكثر بمعالجة الية للمعطيات تنفيذا لبرنامج معين

ج-معطيات معلوماتية : اي عملية عرض للوقائع او المعلومات او المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شانها جعل انظمة معلوماتية تؤدي وظيفتها .

د-مقدمو الخدمات :

1-اي كيان عام او خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/او نظام للاتصالات .

2-واي كيان اخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة او لمستعمليها.

-ه-المعطيات المتعلقة بحركة السير : اي معلومات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الاخيرة باعتبارها جزء ا في حلقى اتصالات ، توضح مصدر الاتصال ، والوجهة المرسل اليها ، والطريق الذي يسلكه ، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة .

و-الاتصالات الالكترونية :اي تراسل او ارسال او استقبال او علامات او اشارات او كتابات او صور او اصوات او معلومات مختلفة بواسطة اي وسيلة الكترونية .

ومما سبق فالجريمة المعلوماتية هي الجرائم الماسة بأنظمة المعالجة الالية للمعطيات المتواجدة في منظومة معلوماتية والمقدمة من قبل مقدمو الخدمات والمنصوص عليها القانون رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات ، المعدل والمتمم بصفة خاصة وبصفة عامة في باقي القوانين .

وكمثال على ذلك نص قانون الجمارك الجزائري رقم 79-07 المؤرخ في 21 يوليو 1979 المتضمن قانون الجمارك في المادة 325 مكرر من القانون رقم 17-04 المتضمن تعديل قانون الجمارك[1]. حيث تنص على مايلي :

[1]-القانون رقم 17-04 المؤرخ في 16 فيفري 2017 ، المتضمن تعديل قانون الجمارك رقم 79-07 ، الجريدة الرسمية للجمهورية الجزائرية ،العدد 11 بتاريخ 19 فيفري 2017 .

"تعد جنحة من الدرجة الثانية الافعال الاتية :...- كل فعل تم باستعمال الوسائل الالكترونية وادى الى الغاء او تعديل او اضافة معلومات او برامج في النظام المعلوماتي للجمارك ، تكون نتيجته التملص التملص او التغاضي عن حق او رسم او اي مبلغ اخر مستحق او الحصول بدون اي وجه حق على اي امتياز اخر ...

يعاقب على هذه الجرائم بما يأتي :

-مصادرة البضائع محل الغش والتي تخفي الغش

-غرامة مالية تساوي ضعف قيمة البضائع المصادرة -الحبس من ستة (06) اشهر الى سنتين (2)".

وهناك من يعرف الجريمة المعلوماتية على انها :"فعل ضار يستخدم الفاعل نظاما حاسوبيا او شبكة حاسوبية للوصول للبيانات و البرامج بغية نسخها او حذفها او تزويرها او تخريبها او جعل غير صالحة او حيازتها او توزيعها بصورة غير مشروعة "[1].

بالإضافة لما سبق فالمشرع الجزائري خص الافراد الطبيعية بحماية معطياتهم الشخصية من خلال القانون رقم 18-07 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[2].حيث نص في المادة الثالثة منه على تحديد بعض المفاهيم والمصطلحات: المعطيات ذات الطابع الشخصي ، الشخص المعني ،معالجة المعطيات ذات الطابع الشخصي ، موافقة الشخص المعني ، المعالجة الالية ،معطيات حساسة ، الاتصال الالكتروني ...وغيرها .

فالجريمة المعلوماتية في هذا الصدد هي كل مساس بمعالجة للمعطيات ذات الطابع الشخصي بصورة الية (نجد ان المشرع اضاف كلمة او يدوية) ،عن طريق الاتصال الالكتروني بإرسال او تراسل او استقبال علامات او اشارات او كتابات او صور او اصوات او بيانات او معلومات مهما كانت طبيعتها عن طريق الاسلاك او الالياف البصرية او بطريقة كهرومغناطيسية ، او تقديم معطيات من قبل مقدم الخدمات سواء كان كيانا عاما او خاصا يقدم لمستعمل خدماته

---

[1]-احمد بن خليفة ،حفوظة الامير عبد القادر ، الجريمة الالكترونية واليات التصدي لها ، مجلة الامتياز لبحوث الاقتصاد والادارة ،المجلد 1 ، العدد 1 ،جوان 2017 ، ص 155 .

[2]-القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ،الجريدة الرسمية للجمهورية الجزائرية ، العدد 34 ، بتاريخ 10 يونيو 2018 .

القدرة على الاتصال بواسطة منظومة معلوماتية /او نظام للاتصالات او اي كيان اخر يقوم بمعالجة او تخزين المعطيات لفائدة خدمة الاتصال .[1]

المطلب الثالث :التعريف الفقهي للجريمة المعلوماتية

تعددت الآراء الفقهية وتضاربت حول مفهوم الجريمة المعلوماتية فمنهم من يعرفها استنادا لموضوعها ومنهم من يرجعها لطبيعة الوسائل المستخدمة وجانب اخر ينظر اليها ويعرفها بالنظر للجاني باعتباره يمتلك خبرات فنية في مجال الحاسوب والانترنيت ومنهم من ضيق في مفهوم الجريمة المعلوماتية ومنهم من وسع في ذلك .

فمن انصار الاتجاه الضيق لفكرة الجريمة المعلوماتية نجد الفقيه الفرنسي (mass) على انها : "الاعتداءات القانونية التي يمكن ان ترتكب بواسطة المعلوماتية بغرض تحقيق الربح ".كما عرفها الفقيه (كلاوس تايدومان) بانها :" كافة اشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الالي ".

اما انصار الاتجاه الواسع للجريمة المعلوماتية فيرى الفقيهان (Credoو Michel) الى ان جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة وكذا حالات الولوج غير المصرح به لحاسب الغير او بياناته ويمكن ان تمتد الى تزيف المكونات المادية والمعنوية للحاسب او حتى سرقة الحاسب في حد ذاته واي من مكوناته [2]

ويعرفها الفقيه (Tiédemen) بانها :" كل اشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب "

---

[1]-المادة 6 من القانون رقم 18-07 ، مرجع سابق ، على مجموعة من الاستثناءات في مجال حماية المعطيات حيث نصت على :

"تستثنى من تطبيق المعطيات ذات الطابع الشخصي :

1-المعالجة من طرف شخص طبيعي لغايات لا تتجاوز الاستعمال الشخصي او العائلي شرط عدم احالتها للغير او نشرها.

2-المحصل عليها والمعالجة لمصلحة الامن والدفاع الوطنيين

3-المحصل عليها والمعالجة لأغراض الوقاية من الجرائم ومتابعة مرتكبيها وقمعها وتلك المحتواة في قواعد البيانات القضائية التي تخضع الى النص الذي احدثت بموجبه ولأحكام المادة 10 من هذا القانون ".

[2]- طرشي نورة ، مكافحة الجريمة المعلوماتية ، مذكرة من اجل الحصول على شهادة الماجيستر في القانون الجنائي ، جامعة الجزائر 1 ، كلية الحقوق ، 2012-2013 ، ص 6 .

ويستنتج من هذه التعاريف انه متى استخدم الحاسب في الاجرام تعد الجريمة جريمة معلوماتية.

وجانب من الفقه من ينظر اليه من زاوية تقنية او فنية ،حيث يعتبرون الجريمة المعلوماتية "هي نشاط اجرامي تستخدم فيه تقنية الحاسب بطريقة مباشرة او غير مباشرة ، كوسيلة او هدف لتنفيذ العمل الاجرامي المقصود "[1].

وهناك من ينظر الى معيار محل الجريمة ووسيلة ارتكابه وهنا يعد الحاسب هو الضحية والوسيلة، حيث يعرف الفقيه smedinghoff الجريمة المعلوماتية على انها :"اي ضرب من النشاط الموجه ضد او المنطوي على استخدام نظام الحاسوب "[2].

و من الفقهاء الذين نادوا بمعيار موضوع الجريمة الاستاذ rosenblatt والذي عرفها بانها :"نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصل الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه". ومن انصار المعيار الذين نادوا بوسيلة الجريمة كأساس للجريمة المعلوماتية الاستاذ جون فروست وعرفها كما يلي :"فعل اجرامي يستخدم الحاسب فيه كأداة رئيسية "، اما ويعد الفقيه stein schjglberg من اهم الذين نادوا بتعريف الجريمة المعلوماتية بالنظر للشخص الفاعل والذي يتسم بصفات اهمها توفر المعرفة التقنية لفاعلها[3].
ومما سبق فالفقهاء يعتمدون على عدة معايير لتحديد مفهوم الجريمة المعلوماتية اما بالاستناد على موضوع الجريمة او وسيلة ارتكاب الجريمة واما بالنظر للشخص الفاعل.

المطلب الرابع :التعريف على ضوء الاتفاقيات الدولية

ان مسالة الجريمة الالكترونية لم يقتصر صداها على القانون الداخلي بل امتد ليشمل العديد من الدول ، لما لها من اهمية في حفظ الامن المعلوماتي وتثبيت المعطيات وحماية الحسابات والاشخاص والممتلكات ، كما انها لا تعترف بالحدود فقد يكون الفاعل في دولة والضحية في دولة اخرى كاختراق الحسابات ، تحويل الاموال وكذا في المعاملات الإلكترونية كالتعاقد عبر الوسائط الالكترونية لاسيما في مجال التجارة الالكترونية ، وامام هذه التطورات التكنولوجية

---

[1]-عادل يوسف عبد النبي الشكري ، الجريمة المعلوماتية وازمة الشرعية الدولية ،مركز دراسات الكوفة ،العدد7، 2008 ،ص 112 .

[2]-رحموني محمد ، مرجع سابق ، ص 437 .

[3]-احمد اسامة حسنية ،الجريمة الالكترونية بين الشرعية الجنائية والاجرائية ،مجلة جامعة الازهر ،غزة ، عدد خاص بكلية ملتقى الحقوق الخامس المحكم ، المجلد 19 ،ص 5 وما بعدها .

الناتجة عن استخدام الانترنيت والحاسب ،سارعت الدول لعقد الاتفاقيات الدولية لتحديد هوية الجاني والقبض عليه ومن هنا يتجسد مبدا التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، ومن بين الاتفاقيات الدولية ما يلي[1]

ا-معاهدة بودابست لمكافحة جرائم الانترنيت

ب-المعاهدة الاوروبية لمكافحة جرائم الانترنيت

ج-معاهدة برن لحماية المصنفات الادبية والفنية

د-معاهدة تريبس

اما على المستوى العربي، فقد قامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة تقنية جرائم المعلومات وذلك بتاريخ 21ديسمبر 2010 ،والتي دخلت حيز التنفيذ بعد مصادقة الرئيس المصري عليها في سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها [2]

فالملاحظ على هذه الاتفاقيات سواء الثنائية او الجماعية او الاقليمية لم تعط تعريف موحد للجريمة الالكترونية فكل مجموعة تنظر اليها من زاوية معينة ومحددة وخاصة بها ، حيث اكتفت بتحديد طرق التعاون في مجال مكافحة هذا النوع من الجرائم المستحدثة نظرا لحجم الضرر الذي قد تلحقه بالضحية ودون ترك اي دليل في بعض الاحيان والسعي لسن تشريعات وتكييفها داخل الانظمة الداخلية عل ان تتماشى والانظمة الدولية بغية توحيد الجهود[3]

المحـــــــــــــور الثاني : سمات وخصائص الجريمة المعلوماتية

تعد الجريمة المعلوماتية من الجرائم الحديثة فهي تتميز بمجموعة من السمات تميزها عن غيرها من الجرائم التقليدية وذلك بالنظر الى الوسائل التقنية المستخدمة كالحاسب الالي والدراية الكافية من قبل الجاني بتقنية المعلومات حيث اصبحنا امام ما يعرف بالمجرم المعلوماتي. وتكمن هذه الخصائص فيما يلي : طريقة التنفيذ واسلوب الارتكاب ،صعوبة الاثبات ،الاكتشاف ،عالمية الجريمة المعلوماتية والمجرم المعلوماتي .

المطلب الاول : طريقة التنفيذ واسلوب الارتكاب

---

[1]-سعيداني سلامي ،تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (واقع ومقاربات)،مجلة الاستاذ الباحث للدراسات القانونية ،المجلد الاول ، العدد العاشر، جوان 2018 ، ص 199 وما يليها .

[2]-احمد خليفة ،حفوظة الامير عبد القادر ،مرجع سابق ،ص 162 .

[3]-معاشي سميرة ، مرجع سابق ، ص 414 .

وهذا لكون الجريمة المعلوماتية تميز بالطابع التقني ولصعوبة الاثبات فيها نظرا لسهولة وسرعة فسخ ومحو الدليل في وقت سريع ، حيث يتم التنفيذ بسرعة وتكفي ضغطة واحدة من الهاتف او الحاسب الالي ان تمر البيانات او تنقلها او تقوم بتحويل الحسابات وغيرها ، وهذا كله يتم عن بعد اي دون وجود الفاعل في مسرح الجريمة [1]. وبالتالي فهي تختلف عن الجرائم التقليدية التي في غالب الاحيان تتطلب العنف والمجهود البدني لارتكابها الضرب والقتل والتحطيم والكسر... عكس اسلوب تنفيذ الجريمة المعلوماتية فهي تتم بذكاء وسرعة مع قدرة فنية و تقنية في التعامل مع الحاسب والانترنيت [2] .

المطلب الثاني : صعوبة الاثبات والاكتشاف:

ان الجرائم الواقعة على الانترنيت جرائم مخفية ، وتميز عن غيرها من باقي الجرائم بعدم استخدام المجني للعنف كما في الجرائم العادية حيث يتم ارتكاب الجريمة المعلوماتية بنقل معلومات او تخريب معطيات من جهاز لآخر سواء كان حاسبا او هاتفا او من قبل احدى الاجهزة الذكية التي تتصل بالأنترنيت وبالشبكة المعلوماتية ،وبالتالي سهولة تدمير الدليل لعدم وجود خبرات في مجال المعلوماتية لأجهزة التحقيق سواء كانت شرطة او غيرها [3].

كما انها صعبة الاكتشاف لأنها تنفذ بواسطة وسائل دقيقة ومتطورة فهي تميز بكونها مستترة ومتخفية في غالب الاحيان و لا تترك اي دليل كتابي او مادي واضح لتنفيذها بوسائط الكترونية تؤثر على الضحية اما في مال او شخصه اما بالسرقة او التعديل او الاتلاف او التحطيم والسبب في عدم ترك اثر او دليل خارجي وقدرته على محوه في اقل من ثانية [4].

المطلب الثالث : عالمية الجريمة المعلوماتية :

بمعنى هي جرائم تتخطى الخطوط الجغرافية للدول ، فبظهور شبكة المعلومات وربط العالم بشبكة الاتصالات ، اصبح نقل المعلومات عبر الدول بوسائل غير مرئية وغير ملموسة وهذا من خلال

---

[1]-عبد العال الديربي ومحمد صادق اسماعيل ، مرجع سابق ،ص 54-55 .

[2]-مولاي براهيم عبد الحكيم ،الجرائم الالكترونية ،مجلة الحقوق والعلوم الانسانية ،جامعة زيان عاشور الجلفة –الجزائر ، المجلد الثاني ،العدد 23 ،ص 214 .

[3]- عبد العال الديربي ومحمد صادق اسماعيل مرجع سابق ، ص 56 .

[4]-رحموني محمد ، مرجع سابق ، ص 441 .

الحاسب الالي و الانترنيت في نقل وتبادل المعلومات وبالتالي تأثر العديد من الدول بالجريمة المعلوماتية في وقت واحد ، وهو ما يميز الجريمة المعلوماتية عن الجرائم التقليدية [1] .

فغالبا ما تكون الجريمة المعلوماتية في دولة والجاني في دولة اخرى وهذا بفعل الانترنيت التي تقضي على الحدود بين الدول وهو ما يؤدي الة المساس بثقافة الدولة المجني عليها او التأثير على دينها او نظامها المعلوماتي والسياسي [2].وبالتالي يثور اشكال حول مجال الاجراءات والاختصاص في التحقيق والتفتيش في الجرائم العابرة للدول .

المطلب الرابع : المجــــرم المعلوماتي :

ان الاجرام التقليدي عادة ما يكون عن طريق العنف او الاكراه او الضرب ...، اما الاجرام المعلوماتي فنجد ان المجرم المعلوماتي يمتاز بدرجة ذكاء لا نه يتعامل مع اجهزة متطورة وتقنية عالية في ميدان المعلوماتية والحاسب ، وكذا الهواتف الذكية وعليه فالمجرم المعلوماتي يمتلك درجة من العلم والمعرفة وبالتالي مرتكبو هذه الجرائم هم اما :

-مخترقون او متطفلون وهو ما يطلق عليهم "هاكرز"-مجرمو الكومبيوتر المحترفون -فئة صغار السن وحبهم الاطلاع والاستكشاف -الحاذقون وهم من تحركهم الرغبة في الانتقام و الثأر ... ويتميز -المجرم المعلوماتي- بمجموعة من السمات ويرمز اليها الاستاذ باركر " Parker" بكلمة S.K.R.A.M وهي تعني : المهارة SKILL ، المعرفة Knowledge ، الوسيلة Resources ، السلطة Anthority ، الباعث Motives

وهناك من يضيف سمات اخرى كالذكاء وانه متخصص في هذا النوع من الاجرام ، فالمجرم المعلوماتي يعتبر ذكيا في التعامل مع اجهزة الحاسوب والشبكات ، وقد يكون الاجرام المعلوماتي عنيفا ويتجسد ذلك في اتلاف الحاسب الالي او احد مكوناته ، وقد يكون الاتلاف بوسائل عادية دون الحاجة للعنف المسح الكلي او الجزئي للمعلومات والبيانات والمعطيات [3].

و يعد المجرم المعلوماتي محترفا في تنفيذ جرائمه عن طريق الكومبيوتر وبالتالي امتلاك الدقة والاحترافية للتوصل لمعطيات الغير بمسحها او تخريبها او الولوج اليها [4].وقد يرتكب هذه الافعال

---

[1]- نائلة عادل ، محمد فريد قورة ، جرائم الحاسب الالي الاقتصادية -دراسة نظرية و تطبيقية ، منشورات الحلبي الحقوقية ،سنة 2005 ، ص 50

[2]-عبد العال الديربي و محمد صادق اسماعيل ، مرجع سابق ، ص 55-56 .

[3]-سامى على حامد عياد ،مرجع سابق ، ص 49 .

[4]-عبد العال الديربي و محمد صادق اسماعيل ،مرجع سابق ،ص 59 .

الاجرامية لحسابه الخاص وقد تكون لحساي هيئات اخرى الشركات والمؤسسات الخاصة تعمل في مجال المعلوماتية او اي قطاع اخر[1].

وتضيف الاستاذة هدى حامد القشوش خاصية اخرى وهي خاصية التعود وهذا باعتبار الكثير من الحالات تبقى بمنأى عن المساءلة الجنائية لصعوبة اثباتها والتوصل للمجرم المعلوماتي ، وبالتالي شعور المجرم بالراحة والاقدام من جديد على نفس الافعال الاجرامية في البيئة المعلوماتية الى حد وصوله للاعتزاز بنفسه والاغترار[2] .

ومما سبق فان الجريمة المعلوماتية تتميز بخصائص تميزها عن الجرائم التقليدية وهذا لعدة اسبا ب منها :

-عدم ترك اي اثر خارجي بصورة مرئية او كتابية

-تميزها بالطابع السلمي اي تتم دون عنف او فوضى الا نادرا

-عدم قيام المجني عليه بالتبليغ حتى لا يتم تشويه سمعته او فقد ثقة متعامليه او جمهوره

-ارتكاب هذه الجرائم عن بعد من قبل شخص او اكثر فقد يكون الجاني في دولة والضحية في دولة اخرى

-محو الدليل في اقل من الثانية وفي لمحة بصر من قبل الجاني وبالتالي لا يمكن متابعته بالإدانة .

-ان هذا النوع من الجرائم يصيب الانظمة المعلوماتية ومراكز معالجة المعطيات والبيانات اما بتعديلها او مسحها او تخريبها او تحويلها وسرقتها[3] .

خاتمة :

امام هذه التطورات في ميدان التكنولوجيا الحديثة في برامج الشبكات و الحواسيب و الهواتف الذكية ،وما قدمته من خدمات وسهولة في الاتصال الداخلي والخارجي العابر للحدود ، الا انها ادت في بدورها الى ارتكاب جرائم من نوع خاص نظرا لحداثة الوسائل المستخدمة وكذا بالنظر للجاني الذي يمتاز بخبرة تقنية في مجال المعلوماتية والحاسب ،وبالتالي ازدياد ظاهرة الجريمة المعلوماتية .ومنه يمكننا ان نستنتج ونستخلص مايلي :

---

[1]-احمد حسام حسنية ،الجريمة الالكترونية بين الشرعية الجنائية والاجرائية ،مجلة جامع الازهر –غزة- ،عدد خاص بمؤتمر كلية الحقوق الخامس المحكم ، المجلد 19 ،ص 8 .

[2]-هدى حامد القشوش ،جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية ،القاهرة ،طبعة 1992 ، ص 28 .

[3]-منال هلال المزاهرة ،مرجع سابق ص 308 .

-ان المشرع جرم الافعال التي تشكل جريمة معلومة بموجب قانون العقوبات المعدل والمتمم ، وكذا بموجب بعض القوانين الخاصة كقانون الجمارك رقم 79-07 المعدل والمتمم ، والقانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

-محاولة اعطاء مفهوم موحد للجريمة المعلوماتية وتحديد خصائصها بموجب نصوص قانونية خاصة حسب كل قطاع .

-تفعيل التعاون الدولي في مجال مكافحة الجريمة المعلوماتية لأنها عادة ما تكون عابرة للدول .وعقد الاتفاقيات الدولية والاقليمية .

-القيام بتوعية المستخدمين للحاسب والانترنيت بمخاطر الولوج لبعض المواقع ومحاولة تخريبها او التأثير على قاعدتها البيانية والعقوبة الناتجة عن ذلك .

-تكوين خبراء في مجال المعلوماتية لتحديد صفة المجرمين والكشف عن افعالهم .

المفهوم الفقهي للجريمة المعلوماتية

Juristic concept of information crime

خرشي عثمان باحث دكتوراه

كلية الحقوق والعلوم السياسية

جامعة الدكتور مولاي الطاهر–سعيدة- الجزائر

مقدمة

إنّ العالم كان ولا يزال يشهد منذ منتصف القرن العشرين ثورة معلوماتية على جميع الأصعدة، وذلك للدور البارز الذي تلعبه المعلومات خاصة في الوقت الراهن بحيث أمست قوة لا يستهان بها في أيدي الدول والأفراد، هذا وقد سهل التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصالات من عملية تداول هذه المعلومات بشكل سريع ويسير، وأصبح الاندماج المذهل بين القطاعين يمثل المحور الأساسي الذي تقوم عليه هذه الثورة[1].

وأصبح الحاسوب الآلي من خلالها يلعب دورا رهيبا وخطيرا في الحياة على كوكبنا، فلا أحد يخفى عليه مدى سيطرة الحاسب الآلي على مختلف الأعمال اليومية التي أصبحنا نقضيها بواسطته حتى لا تكاد تجد اليوم عملا على جميع الأصعدة وليس للحاسوب دور فيه[2].

و بذلك فإنّ الانتشار والاستخدام الكبيرين للكمبيوتر والانترنيت جلبا معهما مجموعة من الجرائم لم تكن معروفة من قبل تدعى بجرائم الكمبيوتر والانترنيت أو كما يطلق عليها البعض بجرائم الياقات البيضاء، هذه الجرائم

أصبحت منتشرة جدا وتستهدف الإضرار بالبيانات والمعلومات والبرامج بكافة أنواعها مع ازدياد عمليات القرصنة من جانب "الهاكرز"، كما أنها تميز بنشأتها في الخفاء ومسببة في خسائر فادحة لبعض المؤسسات وصلت لملايين الدولارات[3].

---

[1] نهلا عبد القادر المومنى، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2008، ص13.

[2] محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، الأردن، 2010، ص142.

[3] عماد مجدي عبد المالك، جرائم الكمبيوتر والإنترنيت، دار المطبوعات الجامعية، دون طبعة، الإسكندرية، مصر، 2011، ص5.

لذا فإن ّالاعتداء على الكمبيوتر بصورة عامة أو على جزء من أجزائه قد يلحق بالشخص المعتدى عليه طبيعيا كان أو اعتباريا خسائر مالية أو معنوية، خاصة مع التطور الدوري لتكنولوجيا المعلومات والذي صاحبه ظهور تقنيات وأساليب مستحدثة فنية ترتكب بها مثل هذه الجرائم[1] من قبل مجرمين محترفين في هذا المجال تتوفر فيهم الخبرة والدراية في علم الحاسوب، سواء كانوا مستخدمين أو مبرمجين أو مجرد هاوين، على أن يكونوا محكومين برغبة جامحة في تحدي كل ما هو جديد ومبتكر، بدليل أنّ عددا ممن تم القبض عليهم أفادوا بمحاضر التحقيقات أنهم قاموا بذلك رغبة منهم في تحدي وقهر الأنظمة المعلوماتية المختلفة، هذا ولا ننسى السبب الرئيسي والمتمثل في الطمع المادي الكبير الذي سوف يكسبوه من وراء ارتكابهم لهذه الجرائم، لهذا كثيرا ما يستهدفون بجرائمهم المعلوماتية المؤسسات المالية الكبيرة وبنوك المال والمعلومات أيضا[2].

إن معضلة الجرائم المعلوماتية في هذا العصر أثارت الكثير من النقاشات الفقهية حول نوعية هؤلاء المجرمين المعلوماتيين وأبرزت دهشة الكثير من العلماء من الأرقام الصادمة التي ألحقها هؤلاء المجرمين من خلال اعتداءاتهم على مختلف النظم المعلوماتية، الأمر الذي حز في نفسي أن أتطرق من خلال هذا البحث إلى تبيان أصناف وسمات هؤلاء المجرمين مع ذكر بعض الاعتداءات الشهيرة التي اقترفها مجرمين بعينهم، وذلك بعد إعطاء تعريف شامل لهذه الظاهرة المستحدثة وتحديد طبيعتها القانونية معتمدا في ذلك على المنهجين الوصفي والتحليلي من خلال المبحثين التاليين: مفهوم الجريمة المعلوماتية (المبحث الأول)، و أصناف المجرمين المعلوماتيين (المبحث الثاني) .

المبحث الأول: مفهوم الجريمة المعلوماتية

إنّ مفهوم الجريمة المعلوماتية يقودنا لضرورة معرفة مختلف التعريفات التي جاءت حولها والتي تعددت بتعدد نوع وطبيعة مصدرها من فقهية وتشريعية، ويقودنا أيضا لتبيان الطبيعة القانونية لهذه الجريمة التي تختلف من مشرع لآخر، بالإضافة إلى ذكر أهم الخصائص التي تميز بها عن غيرها من الجرائم التقليدية الأخرى، وكل هذا سيتم تفصيله من خلال المطالب الآتية.

المطلب لأول: تعريف الجريمة المعلوماتية

[1] ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، دون طبعة، الإسكندرية، مصر، 2012، ص6.

[2] عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، الأردن، 2014، ص131.

لقد تعددت التعريفات التي جاءت حول الجريمة المعلوماتية من تشريعية وفقهية، هذه التعريفات اختلفت باختلاف مصدرها واختلاف الموقع الذي ينظر إليه لهذه الجرائم، وهي الجريمة التي تعددت مسمياتها من جريمة إلكترونية وجرائم الحاسوب الآلي وجرائم التكنولوجيا الحديثة إلى غيرها من المسميات الأخرى والتي تدخل كلها في المجال المعلوماتي الواسع والشاسع بطبيعته.

الفرع الأول: التعريف التشريعي للجريمة المعلوماتية

لقد أصدرت مختلف التشريعات المقارنة تعريفات حول الجريمة المعلوماتية والتي سنبرز بعضها من خلال الآتي:

فهذا المشرع السعودي عرفها من خلال نص المادة 01 من نظام مكافحة جرائم المعلوماتية بأنّها: " أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام "[1].

وكذا المشرع الكويتي من خلال المادة 1 من قانون مكافحة جرائم تقنية المعلومات رقم 63 بأنّها : " كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"[2].

وكذلك المشرع الأمريكي عرفها بأنها: "الاستخدام الغير مصرح به لأنظمة الكمبيوتر المحمية أو ملف البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة "[3].

أمّا المشرع الجزائري فلقد جاء تعريفه لها من خلال القانون[4] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها: "جرائم المساس بأنظمة

---

[1] هيئة الاتصالات وتقنية المعلومات، نظام مكافحة جرائم المعلوماتية، عن موقع https://www.citc.gov.sa/ar/ ، تاريخ الإطلاع 2020/03/23.

[2] قانون رقم 63 لسنة 2015 الكويتي في شأن مكافحة جرائم تقنية المعلومات، عن موقع https://www.e.gov.kw/ ، تاريخ الإطلاع 2020/03/23.

[3] أيمن عبد العال، الجرائم الإلكترونية في التشريع الفلسطيني، عمل مقدم لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية غزة فلسطين، 2013، ص7.

[4] قانون رقم 04/09 المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

الملاحظ من خلال التعريفات السابقة أن الجريمة المعلوماتية تنوعت تعريفاتها من مشرع لآخر بحسب تنوع مركز وموقع مصدرها وبحسب نوع الجرائم المعلوماتية الشائعة في منطقة مصدرها، وهو ما فسح المجال للفقه من أجل إيجاد وإعطاء تعريف شامل وموحد للجريمة المعلوماتية وهو الأمر الذي لم ينجحوا فيه بعد، فكانت تعريفاتهم متنوعة هي الأخرى والتي جاء بعضها كالآتي.

الفرع الثاني: التعريف الفقهي للجريمة المعلوماتية

لقد عرفت عملية إيجاد تعريف للجريمة المعلوماتية عدة جهود من قبل الفقهاء الذين اختلفت آراءهم واتجاهاتهم، فكان لرأي أن عرفها بأنّها : " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى" وكذلك بأنّها : " الجريمة التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط"[1].

وفي اتجاه ورأي آخر عرفها بأنها : " كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها"، ويرى كذلك آخرون بأنّها: " كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية"[2].

هذا وقد عرفها كذلك خبراء في المنظمة الأوروبية للتعاون والتنمية الاقتصادية بأنها: " كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها"، وكذلك عرفها مكتب التقنية بالولايات المتحدة الأمريكية بأنها:"الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[3].

وككل فبالرغم من الجهود المبذولة من قبل العديد من الفقهاء في عملية إيجاد تعريف دقيق وموحد للجريمة المعلوماتية فإن محاولاتهم كلها باءت بالفشل بدليل انقسامهم بين اتجاهين، اتجاه

---

[1] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، دون طبعة، الإسكندرية، مصر، 2008، ص42.

[2] محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنيت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2004، ص9.

[3] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، دون طبعة، الإسكندرية، مصر، 2015، ص93.

ضيّق من نطاقها كما هو الحال بالنسبة للتعريفين السابقين الأول والثاني، واتجاه آخر وسع من نطاقها كما هو الحال بالنسبة للتعريفات الأخيرة بحيث أن لكل متبني اتجاه ورأي ما يبرر ويفسر ذلك.

المطلب الثاني: طبيعة وخصائص الجريمة المعلوماتية

تحدد الطبيعة القانونية للجريمة المعلوماتية بتحديد الطبيعة القانونية للمعلومات، هذه للأخيرة التي يختلف منظورها من مشرع لآخر ومن فقيه لآخر، كما تحدد كذلك بخصوصيات هذه الجريمة وما تميز به من خصائص مقارنة بالجرائم التقليدية الأخرى والتي يلعب فيها الجاني دورا كبيرا مهما باعتبارها منبع وسبب مباشر للجريمة المعلوماتية.

الفرع الأول: الطبيعة القانونية الخاصة للجريمة المعلوماتية

تتغير طبيعة الجرائم المعلوماتية وتتنوع بحسب طبيعة السلوك الإجرامي فقد تكون هذه الجرائم جرائم أموال كتزييف العملة باستخدام الحاسب الآلي، وقد تكون جرائم أشخاص كجرائم السب والقذف الواقعة في الوسائط الإلكترونية، كما قد تكون الجرائم المعلوماتية جرائم أمن دولة وجرائم مخلة بالنظام والآداب العامة وكذلك جرائم اقتصادية، لذلك فاعتبار الجرائم المعلوماتية كجرائم أشخاص أو جرائم أموال أو جرائم اقتصادية يعني الإقرار بالطبيعة الخاصة لهذه الجرائم مما يقتضي سن تشريعات خاصة بها[1].

لذلك فإنّ التطور السريع في مجال المعلوماتية قد يفسح المجال لظهور جرائم إلكترونية جديدة لم تكن معروفة من قبل مما يحتم ضمها إلى نطاق القانون الجنائي الذي يبقى عاجزا عن مواكبة التطور المعلوماتي، وحتى هذه الجرائم فهي ذات طبيعة خاصة من حيث تكييفها القانوني، خاصة وأن النصوص التقليدية وضعت وفق معايير مادية عكس الحقوق الشخصية في شبكة المعلومات التي ترد على نتاج الفكر البشري المتعلق بشخص المرء وأمواله وممتلكاته، هذه النصوص التي تثير مشاكل عديدة في تطبيقها على الجرائم المعلوماتية في مقدمتها مسألة الإثبات أين يمكن للجاني محو أدلة الإدانة وتدميرها في وقت سريع[2]، وحتى في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال فقد تكون البيانات التي يجري البحث عنها مشفرة، ومما يزيد من

---

[1] أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، الأردن، 2014 ص95.

[2] علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب، الطبعة الأولى، طرابلس، لبنان، 2006،ص322.

صعوبة الأمر حالة ملاحقة الجناة المقيمين في دولة أخرى لا تربطها أية اتفاقية معها والتي تحقق فيها السلوك الإجرامي أو جزء منه.

أما الجزائر ومن خلال التعديل الدستوري[1] ل1996 فقد تطرق للجريمة المعلوماتية بصفة عامة أين حمى حرمة حياة المواطن الخاصة وحرمة شرفه من أي انتهاك وضمن له سرية مراسلاته واتصالاته الخاصة بكل أشكالها ضمن نص المادة 39 منه، بعدها جاء دور المشرع الجزائي الجزائري فنظم الجريمة المعلوماتية في قانون العقوبات[2] ضمن المواد 394 مكرر إلى 394 مكرر7 والتي جاء بها في قسم خاص باسم المساس بأنظمة المعالجة الآلية للمعطيات أين اتبع اتجاها ضيقا من خلال تحديده لبعض الأفعال التي تعد من قبيل الجريمة المعلوماتية، إلى حين تداركه للأمر بإصداره للقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أين وسع من نطاقها لتشمل الأفعال المجرمة السابقة وفق قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها نظام معلوماتي أو نظام للاتصالات الإلكترونية، لذا فإن من يرتكب أحد هذه الأفعال وتوافرت فيه جميع أركانها الخاصة يعتبر مجرما معلوماتيا في نظر المشرع الجزائري.

الفرع الثاني: خصائص ومميزات الجريمة المعلوماتية

تميز الجريمة المعلوماتية بطبيعة خاصة ميزتها عن غيرها من الجرائم التقليدية الأخرى وذلك لارتباطها بتقنية وتكنولوجيا المعلومات، الأمر الذي أضفى على هذا النوع من الجرائم بعض الخصائص والمميزات التي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح هو الآخر يعرف بالمجرم المعلوماتي[3]، هذا الأخير الذي يلعب دورا جوهريا في هذا النوع من الجرائم ويعد سببا رئيسيا في ظهور هذا النوع الخطير من جرائم.

إن الطبيعة الخاصة للجريمة المعلوماتية تفرز مجموعة من الخصائص تمتع بها هذه الجريمة والتي تميزها عن غيرها من الجرائم التقليدية الأخرى وتمثل هذه الخصائص في:

- الجريمة المعلوماتية جريمة عابرة للحدود وذلك لعالمية شبكة الانترنيت بحيث يمكن ارتكابها من مسافات بعيدة أين لا يتواجد المجرم المعلوماتي في مسرح الجريمة، فالجاني فيها يستطيع

[1] مرسوم رئاسي رقم 438/96 المؤرخ في 7 ديسمبر 1996 المتضمن التعديل الدستوري الجزائري.

[2] قانون 15/04 المؤرخ في 10 نوفمبر 2004 المتمم للأمر 156/55 والمتضمن قانون العقوبات الجزائري.

[3] خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2018، ص26.

ارتكاب فعله في دولة على أن يحقق نتائج جرمه في دولة أخرى وهو ما يزيد من صعوبة اكتشافها وإثباتها.

- صعوبة إثبات الجريمة المعلوماتية لعدم تركها لأي آثار مادية بعد ارتكابها، وتحتاج لخبرة فنية خاصة ملمة بتقنيات الكمبيوتر ونظم المعلومات، كما تعتمد على الخداع في ارتكابها والتضليل في التعرف على مقترفيها، هذا ويصعب الاحتفاظ الفني بدليل هذه الجريمة فالمجرم فيها ستطيع في ظرف وجيز جدا محو وتحريف وتغيير البيانات[1].
- الجريمة المعلوماتية سهلة الارتكاب فهي لا تحتاج إلى أدنى مجهود عضلي ولا تحتاج إلى سلوكيات مادية متعددة لتحقيق النتيجة فيها، فإذا ما توفرت التقنية اللازمة والوسيلة المناسبة للمجرم المعلوماتي يستطيع ارتكابها بسهولة دون عناء جهد ووقت[2].
- الجريمة المعلوماتية مرتكبها يتمتع بخصوصيات أي صفات مميزة من حيث الثقافة والعلم التكنولوجي فالمجرم في هذا النوع من الجرائم ليس عاديا ويتميز بفئاته وأنماطه المختلفة والتي كان الباعث والدافع دورا في تنوعها[3] والتي أدت بهم لسلك طريق هذا النوع من الإجرام، هذه الأنماط والدوافع سيتم إيضاحها من خلال المبحث التالي.

هذا ويعتبر تعذر تحديد عنوان المجرم المعلوماتي من بين أحد أهم المسائل الشائكة التي تساهم في عرقلة عملية التحقيق في هذا النوع من الجرائم، والمجرم فيها يتميز بذكاء فائق الأمر الذي يمكنه من التخطيط الجيد لجريمته قبل الإقدام عليها وإحاطتها بأساليب وتدابير أمنية وتدابير حماية فنية تحول دون كشف أمره وكشف الدليل من قبل أجهزة الاستدلال والتحقيق[4].

المبحث الثاني: أصناف المجرمون المعلوماتيين

إنّ الجريمة المعلوماتية باعتبارها أحد الجرائم المستحدثة على الصعيد الدولي تميز بسهولة وسرعة ارتكابها وببساطة الوسائل المساعدة في اقترافها من قبل مجرمين محترفين في المجال المعلوماتي،

---

[1] خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2007، ص324.

[2] أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق، ص97.

[3] طعباش أمين، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، مصر، 2015، ص23.

[4] براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، عمل مقدم لنيل شهادة الدكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، الموسم الجامعي 2018/2017، ص201 و206.

أغلبهم يسعون من خلال اعتداءاتهم إلى الحصول على مطامع مادية بطريقة يسيرة دون عناء وتعب متجاهلين آثار وحجم الخسائر التي من الممكن أي يلحقوها على الشخص المعتدى عليه طبيعيا كان أو اعتباريا.

المطلب الأول: أصناف المجرمون المعلوماتيين

لقد عرفت الجريمة المعلوماتية منذ ظهورها إلى يومنا هذا عدة أصناف من المجرمين المعلوماتيين، هذه الأصناف تعددت بتعدد الاعتداءات وباختلاف دوافع ورغبات كل مجرم، هذا الأخير الذي يمتلك صفات وخصائص تميزه عن غيره من المجرمين الآخرين وتؤهله لارتكاب هذا النوع من الجرائم.

الفرع الأول: القراصنة المعلوماتيون

غالبا ما يحتوي النظام المعلوماتي على بيانات حساسة، وإذا كان هذا النظام متصل بشبكة الإنترنيت قد يحاول قرصان ما أن يسرق البيانات الحساسة التي يحتاجها من خلال الشبكة[1]، وهؤلاء القراصنة المعلوماتيون قسمهم أغلب الفقه لصنفين "الهاكرز" و "الكراكرز":

- الهاكرز: يمثلون أبرز المجرمين المعلوماتيين والمتخصصين في نظم المعلومات والبرمجيات، أطلق عليهم اسم الهاكرز من قبيل المدح لقدرتهم الهائلة في التعامل مع شبكات الحاسب الآلي وإتقانهم لمختلف لغات البرمجة المعروفة فهؤلاء المجرمون من بين أصحاب التخصصات العالية والذين لهم الهيمنة الكاملة على تقنية الإلكترونيات وتعود أحداث ظهورهم مع بداية الثمانيات أين تحول عدد من المبرمجين إلى مجرمين متمكنين ومستغلين لخبراتهم وإمكانياتهم لأغراض إجرامية تمثلت جلها في الدخول الغير مصرح به إلى أنظمة الحاسب أو سرقة المعلومات السرية وكسر الحواجز الأمنية الموضوعة لهذا الغرض[2]، ونظرا للمهارة العالية التي يتمتع به هؤلاء فغالبا ما تكون جرائمهم ضخمة وذات أهمية كبرى وما يزيد من الخطورة قلة العناصر الخبيرة القادرة على كشفها، فهذا الصنف من المجرمين قادرين على تعديل وتحويل ونسخ وإضافة أي معلومات

---

[1] Union internationale des télécomunications, ressources sur la législation relative a la cybercriminalité, comprendre la cybercriminalité guide pour les pays en développement, division application TIC et cybersécurité, département des politique et stratégies, secteur du développement des télécomunications de l'UIT , avril2009, p25.

[2] محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، دون طبعة، الإسكندرية، مصر، 2018 ص50.

على البرامج أو على صفحات المواقع الإلكترونية، وبإمكانهم كذلك إتلافها وتغيير محتواها لتحقيق أغراض غير مشروعة[1].

- الكراكرز: كراكرز كلمة مستمدة من الفعل الإنجليزي (crak)، والتي تعني التكسر والتحطيم وهو ما يقوم به هؤلاء المخبرين أين يستعملون مختلف البرامج والتقنيات في محاولتهم لاختراق الأنظمة المعلوماتية بهدف الحصول على المعلومات أو القيام بعمليات تخريبية[2]، هذا الصنف يتشابه مع الهاكرز في قدرتهم الفائقة على الاختراق وتخطي إجراءات وبرامج الحماية إلا أنّهم يقومون بالعبث بالبيانات والمعلومات المخزنة على تلك الحاسبات والشبكات، كما أنهم أخطر من الصنف الأول لأن أفعالهم هذه قد تحدث أضرارا جسيمة ويعودون في الغالب إلى ارتكاب الجريمة مرة أخرى ويعيشون من عائد جرائمهم[3]، ولا يتبنون الأفكار المتطرفة وإنّما الأفكار التي تدر عليهم أرباحا شخصية[4].

الفرع الثاني: المجرمون النوابغ والمحترفون في المجال المعلوماتي

صنفين آخرين من المجرمين المعلوماتين أثارا دهشة ولفتا انتباه العديد من الفقهاء وهما النوابغ الصغار والمحترفون في المجال المعلوماتي:

- الصغار النوابغ في المجال المعلوماتي: وهم الشباب المولع بالمعلوماتية والحاسبات الآلية وجل أفعالهم تمثلت في الانتهاك غير المسموح به لذاكرات الحاسبات الآلية، هذه الفئة مفتونة بالأنشطة الغير مشروعة المبتكرة والمستحدثة ولا تقدر أبدا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم الجرمية وذلك كله بسبب ميلهم فقط للمغامرة والتحدي والرغبة في الاكتشاف فالخطر الذي يواجه هذه الطائفة هو احتمال الانزلاق الذي من الممكن أن يحدث لهؤلاء أين

---

[1] تميم بن عبد الله بن سيف التيمي، الجرائم المعلوماتية في الاعتداء على الأشخاص، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، السعودية، 2016 ص29.

[2] دنخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2016، ص60.

[3] منير محمد الجنبهي، ممدوح محمد الجنبهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، دون طبعة، الإسكندرية، مصر، 2005، ص28.

[4] صغير يوسف، الجريمة المرتكبة عبر الإنترنيت، عمل مقدم لنيل شهادة الماجستير في القانون الدولي العام، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، الموسم الجامعي 2013/2012، ص28.

يمكنهم أن يصبحوا من مجرد هواة صغار للأفعال الغير المشروعة إلى محترفي لأعمال السلب، كما أنهم معرضين للاستغلال من قبل منظمات أو أفراد غير شرفاء[1].

➢ المحترفون المعلوماتيون: هذا الصنف من المجرمين يتميزون بسعة الخبرة والإدراك الواسع لتقنية المعلوماتية وقدر كبير من الذكاء، كما أنّهم يعملون وفق مجموعات إجرامية منظمة والتي عادة ما تخطط للأفعال التي سترتكبها، وهم من أخطر مجرمي المعلوماتية لرغبتهم في تحقيق الكسب المادي لهم أو للجهات التي استخدمتهم في إطار ما يسمى بالجريمة المنظمة وكذلك لرغبتهم في لفت النظر أو فرض معتقدات دينية أو سياسية أو اجتماعية، لذا فهم عادة مجموعة من الأشخاص المتطرفين فكريا يدافعون عن قضية لها علاقة بمصالحهم الشخصية بطريق إلحاق أضرار جسيمة للآخرين[2]، ومثال ذلك الجماعة المتطرفة التي ظهرت في فرنسا باسم منظمة إزالة وتدمير الحاسبات ونظم المعلوماتية (C.L.O.D.O) قامت بعدة اعتداءات في أرجاء أوروبا.

المطلب الثاني: دوافع ارتكاب الجريمة المعلوماتية

لقد ارتكبت العديد من الجرائم المعلوماتية ولا تزال ترتكب إلى يومنا هذا، حتى أن بعضها ضاع صيتها عالميا بسبب ما ألحقته من ضرر وبسبب ما ألحقته من خسائر فادحة للمجني عليهم، وكل هذه الجرائم إلا ولها أسباب متعلقة بشخص الجاني الذي يلجأ لمثل هذه الاعتداءات وفق دوافع ورغبات معينة، أين يتلاعب بالمنظومة المعلوماتية للمجني عليه مغرقا إياه في بحر من الأضرار.

الفرع الأول: دوافع المجرمين المعلوماتيين في ارتكابهم للجريمة المعلوماتية

حتى الآن لا تزال الصورة لم تتضح في شأن ضبط الدوافع التي تؤدي بالمجرم المعلوماتي لسلك مسلك الجريمة نظرا لقلة الدراسات الخاصة بهذه الظاهرة وصعوبة الإلمام بمداها الحقيقي من حيث حجمها[3]، إلا أن هذا لم يمنع العديد من فقهاء الاجتماع إلى ذكر بعض الأسباب التي قد تدفع المجرم المعلوماتي لارتكاب إحدى الجرائم الإلكترونية والتي سنبرز بعضها في الآتي:

---

[1] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنيت، دون طبعة، دار الفكر الجامعي، الإسكندرية، مصر 2007، ص53.

[2] دخلار صلاح بوتاني، المرجع السابق، ص61.

[3] أيمن عبد الله فكري، الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، السعودية، 2015، ص121.

- تحقيق مكاسب مالية بطرق مختلفة كالمساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس وكاستعمال بطاقة سحب آلي مزورة أو منتهية لصلاحية[1]، ويعتبر هذا الدافع من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية نظرا لما يحققه لهؤلاء من ثراء فاحش مقارنة بالجرائم التقليدية الأخرى، وتكون الجريمة عموما التي تستهدف الربح مدفوعة بالجشع[2].
- دافع الانتقام ومثال ذلك قيام محاسب قام بالتلاعب بالبرامج المعلوماتية أين تبدأ أثار جريمته بعد أشهر من رحيله أين سيتم تدمير البيانات الخاصة بحسابات وديون المنشأة، كما قد يكون العمال في قطاع التقنية معرضون لضغوط نفسية ناجمة عن ضغط العمل والمشكلات المالية والتي تدفعهم إلى الانتقام من المنشأة أو رب العمل[3].
- الرغبة في التحدي وإثبات الذات وذلك لأجل تحقيق الانتصار والإحساس بالفخر والمتعة ولذة التفوق على تقنيات الأنظمة المعلوماتية ويتزايد شيوع هذا الدافع لدى فئات صغار السن الذين يمضون وقتا طويلا أمام حواسيبهم في محاولة منهم كسر حواجز أمن أنظمة الحواسيب وشبكات المعلومات[4].

كانت هذه العناصر الثلاثة أبرز الدوافع التي قد تقود المعتدين إلى الإضرار بالنظام المعلومات، مع وجود بطبيعة الحال دوافع أخرى تقود إلى نفس المسلك إلا أنّها بنسب قليلة مقارنة مع الدوافع المذكورة.

الخاتمة

تبقى الجرائم المعلوماتية من أبرز الظواهر الإجرامية المستحدثة على الصعيدين المحلي والدولي، ولازالت في تزايد و تطور مستمر، خاصة مع التطور الهائل والسريع لتقنيات وتكنولوجيا المعلومات الذي أفرز أصنافا جديدة ومتنوعة من مجرمين معلوماتين على جميع المستويات خاصة

---

[1] محمد أمين الرومى، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، دون طبعة، الإسكندرية، مصر، 2004، ص24.

[2] Tamas Gaidosch, la filiere bien structuree de la cybercriminalite, revue finance &developement Washington, USA, juin 2018, p22.

[3] خالد داودي، المرجع السابق، ص40.

[4] طاهر محمود أبو القاسم، الجرائم المعلوماتية صعوبات وسائل التحقيق فيها وكيفية معالجتها، المنظمة العربية للتنمية الإدارية، القاهرة، مصر، 2019، ص44.

الاقتصادية منها، هذه الأصناف والفئات تختلف فيما بينها من حيث الدوافع والرغبات وإن كان أكبر نسبة منها ترتكب هذه الجرائم من أجل الحصول على منافع مادية أو معنوية، ولعل ما يثير العجب أن هذه الأصناف بالرغم من تمتعها بالذكاء والنبوغ في المجال المعلوماتي إلا أنهم يسلكون مسلك هذا النوع من الإجرام المحفوف بالكثير من المخاطر على حياتهم، وغير مبالين بحجم الأضرار والخسائر التي من الممكن أن يحدثوها على ضحايا المعلوماتية.

وعليه ومن خلال ما تم التطرق له في هذه الدراسة خرجنا بمجموعة من النتائج من أهمها أنّ:

- ➢ الجريمة المعلوماتية تبقى في توسع مستمر وموازية للتطور الدوري لتقنيات وتكنولوجيا المعلومات.
- ➢ المجرمون المعلوماتيون تختلف دوافعهم ورغباتهم من مجرم لآخر والتي قد تكون فقط من أجل الترفيه.
- ➢ سمات وصفات المجرمين المعلوماتيين تعود لطبيعة فعل الاعتداء على النظام المعلوماتي.
- ➢ نسبة معينة من المجرمين المعلوماتيين لم يتم كشفهم ولا كشف اعتداءاتهم إلى حد الساعة.

هذا وبالرغم من هذه المعضلة التي باتت تهدد الكثير من الأشخاص الطبيعية والاعتبارية في حياتهم الاجتماعية أو الثقافية أو الاقتصادية، إلا أن العالم لا يزال يزخر بالمقابل على نوابغ ومختصين ومحترفين في مجال المعلوماتية الذين بإمكانهم كشف وإحباط جل هذه الاعتداءات وغالبيتهم ينتمون لمختلف الأجهزة الأمنية والقضائية التي أحسنت توظيفهم، لذا حري بكل دولة متخلفة في مجالها المعلوماتي أن:

- ➢ تقوم وتحسن اقتناص مثل هؤلاء النوابغ والمحترفين في المجال المعلوماتي ليكونوا ذرعا حاميا لها ضد الهجمات والاعتداءات المعلوماتية بكل أشكالها، ولا يتأتى ذلك إلا بتوفير جل الاحتياجات والإمكانيات المادية والمعنوية لهؤلاء حتى تساعدهم في القيام بعملهم على أكمل وجه.

الجريمة الالكترونية بين القيام و التجريم

Cyber crime between doing and criminalizing

د. تياتي مريم استاذ مساعد قسم - ب

معهد الحقوق و العلوم السياسية

المركز الجامعي مغنية - الجزائر

مقدمة :

تغيرت أنماط الجريمة ، فلم تعد الاعتداءات تستهدف النفس والمال فقط ، بل طالت المعلومات وهو ما أصبح يعرف على الساحة الدولية بإجرام ذوي الياقات البيضاء حيث يستطيع المجرمون العصريون ارتكاب أبشع الجرائم ، ليس فقط دون إراقة دماء ولكن أيضا بدون الانتقال من أماكنهم ، بل ترتكب الجريمة في أمن وهدوء ، وهو ما جعل البعض يصفها بالجرائم الناعمة (Crime Soft) فبمجرد لمس لوحة المفاتيح يحدث دمارا وخرابا في اقتصاديات كبرى الشركات ، وهذا النوع من الجرائم ليس مقصورا على منطقة أو دولة معينة ، لكنها مشكلة عالمية[1].

وبذلك الجريمة الإلكترونية تعتبر من الظواهر الحديثة ودلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات والكومبيوتر وقد أحاطت بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها ، ولكن الفقه لم يتفق على تعريف محدد ، بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني[2].

وانطلاقا لما سـلف ذكره، أطـرح تساؤلي هل تشتبه الجريمة الالكترونية مع الجريمة العادية من حيث الأركان و التعريف ؟ وهل جرمها المشرع الجزائري ؟ وللإجابة على هذه التساؤلات اتبعت الخطة التالية:

المبحث الأول: ماهية الجريمة الالكترونية

---

[1] سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني ، كلية الحقوق والعلوم السياسية ، عدد 7،جامعة محمد خيضر بسكرة ، أفريل 2010 ، ص 275 ، 276.

[2] خالد ممدوح إبراهيم ، أمن الجريمة المعلوماتية ، الدار الجامعية ، الاسكندرية ، 2008 ،ص 14 .

سأعالج خلال هذا المبحث ماهية الجريمة الالكترونية، حيث تضمن المطلب الأول تعريفها ولا يكتمل البحث في ماهية الجريمة الالكترونية دون البحث في خصائصها في المطلب الثاني وأركانها في المطلب الثالث.

المطلب الأول: تعريف الجريمة الالكترونية

أعطى الفقهاء للجريمة الالكترونية تعريفا وفقا لمجالين ضيق و واسع ، فوفقا للمفهوم الضيق عرفت على أنها : كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكاب من ناحية لملاحقته وتحقيقه من ناحية أخرى.

حيث يرى الأستاذ mass أن المقصود بالجريمة المعلوماتية " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"[1].

بينما في المجال الواسع عرفت على أنها : كل فعل أو امتناع عمدي ، ينشأ عن الاستخدام الغير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشيـاء المعنوية.

أما المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث[2].

فقد جرم المشرع الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية وبأشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل هذا ما دفعه إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في العاشر من نوفمبر 2004 المتمم لأمر رقم 66-156 المتضمن قانون العقوبات والذي افرد القسم السابع مكرر منه تحت عنوان : المساس

---

[1] نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ماجستير في القانون الجنائي المعلوماتي،دار الثقافة للنشر والتوزيع 1429هـ - 2008 م ، الطبعة الأولى ، الإصدار الأول ـــــ 2008 ، ص 48 .

[2] قانون رقم 09 ـ 04 المؤرخ في 05 أوت 2009 ،يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ، ج ر عدد 47 ،صادر ة بتاريخ 16 /08 / 2009 ، ص 2.

بأنظمة المعالجة الآلية للمعطيات والذي تضمن 08 مواد من المادة 394 مكر ر وحتى المادة 394 مكرر 07[1] .

المطلب الثاني: خصائص الجريمة الالكترونية

تميز الجريمة الالكترونية بطبعة خاصة تميزها عن الجريمة التقليدية ولذا أصبحت هذه الخاصية بهذا النوع من الجرائم عدة سمات وحقائق سواء تعلق الأمر بمرتكبيها أو ما يسمى بالمجرم المعلوماتي أو بالنسبة لحدودها باعتبارها جريمة ذات بعد عالمي[2] .

الفرع الأول : الطابع الدولي للجريمة

من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية ومن اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود ، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة ، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال ، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

الفرع الثاني: الطابع الخاص للجريمة المعلوماتية

تتسم الجريمة المعلوماتية بصعوبة الإثبات و اكتشافها لأن وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها خشية المجني عليهم من فقد ثقة عملائهم ، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة[3].

الفرع الثالث: دافع ارتكاب الجريمة الالكترونية

---

[1] عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق جامعة الاسكندرية ، 2006 ، ص 32.

[2] يونس عرب ، جرائم الكمبيوتر والانترنت ، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ، المركز العربي للبحوث والدراسات الجنائية ، أبو ظبي 10/12/ 2012 ، ص 08 .

[3] نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية ، منشورات الحاتي الحقوقية ،2005 ، ص 49

دافع ارتكاب الجريمة المعلوماتية قد يختلف عن دافع الجريمة التقليدية فقد يكون الدافع مخالفة النظام العام والخروج على القوانين وقد يكون ماديا يراد به اكتساب مبالغ طائلة أو الإهانة وتشهير و الثأر...إلخ يكون دون الاحتكاك المباشر بالمجني عليه[1] .

المطلب الثالث: أركان الجريمة الالكترونية

تتخذ الجريمة المرتكبة عبر الانترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها إلا أن ذلك ال يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي ، فهي تشترك بوجود الفعل غير المشروع و المجرم يقوم بهذا الفعل من خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة، وبالتالي نعمد إلى تبيان مدى انطباق مبدأ الشرعية على الجريمة الإلكترونية في الفرع الأول و نوضح الركن المادي في الفرع الثاني ، لننتهي إلى تحديد الركن المعنوي في الفرع الثالث.

الفرع الأول: الركن الشرعي

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه[2].

فالركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين وهما تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة وعدم خضوع الفعل المرتكب لأي سبب من أسباب الإباحة[3].

الفرع الثاني: الركن المادي

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور و القانون فهذا الاعتداء يكون في ثلاثة أشكال وهي :

أولا/ الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

---

[1] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992، ص 62.

[2] حسن بوسقيعة ، الوجيز في القانون الجزائي العام ، دار هومه ، الجزائر ، ط 10 ، 20111 ، ص 27.

[3] بلعليات إبراهيم ، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري ، الطبعة الأولى ، دار الخلدونية ، الجزائر، 2007 ، ص 95 .

فيكون هذا الشكل من الاعتداء في صورتين و هو ما نص عليه في المادة 394 مكرر من قانون العقوبات الجزائري ، فيكون على صورة جريمة بسيطة تمثل في الدخول أو البقاء غير المشروع و اخرى مشددة تحقق بتوافر الظرف المشدد المتمثل في حصول نتيجة الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

ثانيا/ الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات

المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة داخل النظام ، وهذا راجع إلى تفسير أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام ووظائفه[1].

فقد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية ، فإذا كان الاعتداء مجرد وسيلة فان الفعل يشكل جريمة الاعتداء العمدي على النظام ، أما إذا كان الاعتداء غاية فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

ثالثا/ الاعتداءات العمدية على المعطيات

إن جريمة الاعتداء العمدي على المعطيات جريمة عمدية يتخذ فيها القصد الجنائي بعنصرية العلم والإرادة ، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل ، كما يجب أن يعلم الجاني بان نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ، ويعلم أيضا أنه ليس له الحق في القيام بذلك و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

فلتوافر الركن المعنوي يشترط القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه ، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة[2] .

المبحث الثاني: مكافحة الجريمة الالكترونية في القانون الجزائري

نتيجة للتطور السريع في التكنولوجيا وتقنيات المعلومات (شبكة الانترنت) ، أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية في تطبيقها على الجرائم المستحدثة في ظل التطور الهائل

[1] نائلة محمد فريد قورة ، المرجع السابق ، ص190 .

[2] أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومه الجزائر ، ط 2 ، 2007 ، ص 125.

في أنظمة معالجة المعلومات ونقلها عبر الشبكات، وباتت الحاجة ضرورية لاستحداث قواعد قانونية جديدة لمواجهة هذه الجرائم المستحدثة[1].

المطلب الأول: الحماية في ظل قانون العقوبات

نجد أن المشرع الجزائري تدارك الفراغ القانوني في مجال الإجرام المعلوماتي ولو نسبيا، خصوصا بموجب القانون رقم 04-15 المتضمن تعديل قانون العقوبات، إذ بموجبه جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات .

الفرع الأول: جريمة المساس بأنظمة المعالجة الآلية للمعطيات

بمعنى جريمة الغش المعلوماتي وهو الفعل المنصوص والمعاقب عليه في المواد 394 مكرر إلى المادة 394 مكرر 7 فالمشرع الجزائري لم يعرف لنا نظام المعالجة الآلية للمعطيات،لكن بالرجوع إلى الاتفاقية الدولية الخاصة بالإجرام المعلوماتي قدمت تعريفا للنظام المعلوماتي في مادتها الثانية، وكذلك عرفها الفقه الفرنسي[2].

فالغش المعلوماتي له عدة صور منها : الدخول في منظومة معلوماتية بمعنى الدخول و البقاء أو المساس بمنظومة معلوماتية فعقوبة الاعتداء العمدي على المعطيات الموجودة داخل النظام، وذلك بالحبس من 06 أشهر إلى 03 سنوات وغرامة من 500،000دج إلى 2 000.000 دج وفي حالة حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية تكون العقوبة، الحبس من شهرين إلى 03 سنوات وغرامة من. 5.000.000 إلى 1.000.000 دج .

أو قد يكون الغش المعلوماتي في احدى الصور التي جاءت في نص المادة 394 مكرر 2 من قانون العقوبات الجزائري مثل :

- ✓ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم الغش المعلوماتي.

---

[1] رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان ، 2011 – 2012 ، ص88 .

[2] عرف الفقه الفرنسي جريمة المساس بأنظمة المعالجة الآلية للمعطيات بأنها : (كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية) .

الفرع الثاني: جريمة التزوير المعلوماتي

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي ، الذي يعتبر من اخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسوب الآن فنجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد 214 الى229 التي تشترط المحرر لتطبيق جريمة التزوير ، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من اجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير.

رغم تداركه من خلال القانون 15/04 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على منتوجات الإعلام الآلي ، فلم يستحدث نصا خاصا بالتزوير المعلوماتي ، ولم يتبنى الاتجاه الذي تبنته التشريعات التي عملت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث[1].

المطلب الثاني : الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تواكبا مع التطورات التي عرفتها الجزائر في مجال تطور التقنية و التكنولوجيا ، ولأنها في الغالب أصبحت محلا للجريمة باشر المشرع الجزائري إجراءات جديدة للمواجهة تضمنت إصدار القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، وهو القانون المنظم لفضاء المعلوماتية بصفة عامة ومكافحة المجال الإجرامي المتصل بها من خلال قواعد تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة[2] .

يتكون هذا القانون من 19 مادة موزعة على ستة فصول ، كما يتضمن القانون أحكام خاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها وهي الأفعال الموصوفة بجرائم الإرهاب و التخريب ، والجرائم الماسة بأمن الدولة أو حالة توفير معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام[3].

---

[1] أمال قارة، المرجع السابق، ص 140.

[2] سعيدة بوزنون ، مكافحة الجريمة الالكترونية في التشريع الجزائري،مجلة العلوم الإنسانية، عدد 52 ديسمبر 2019، المجلد ب،ص 50.

[3] رصاع فتيحة، المرجع السابق ، ص 113 .

إن الظاهر من النص يوحي بأن القانون يتضمن انتهاك صارخ للحق في الخصوصية، ولكن الواضح أن هناك ما يبرره في الغالب وهو مضمون المادة 4 من القانون 90-04 التي نصت على أربع حالات يجوز فيها فقط اللجوء إلى هذا الإجراء وذلك بالنظر إلى خطورة التهديدات المحتملة ولأهمية المصلحة المحمية منها :

- ✓ جرائم الإرهاب والتخريب وجرائم ضد امن الدولة .
- ✓ عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية تهدد مؤسسات الدولة أو الدفاع الوطني .
- ✓ لضرورات التحقيق والمعلومات القضائية .
- ✓ في إطار تنفيذ طلبات المساعدات القضائية بين الدول[1].

المطلب الثالث: الحماية في نصوص الملكية الفكرية

اعتمد المشرع الجزائري من أجل حماية المصنفات الفكرية شروطا عامة، تمثل في وجود المصنف ثم عدم مخالفته للنظام العام، وأخرى خاصة وهي وجود ابتكار جديد في المصنف ثم القيام بإيداعه القانوني[2] .

الفرع الأول: مدى خضوع معطيات الحاسب الآلي لنصوص الملكية الصناعية.

رمز حقوق الملكية الصناعية إلى المبتكرات الجديدة كالاختراعات، وقد نضمها المشرع بقانون شهادات المخترعين وبراءات الاختراع .ويرى القائلون بالحماية لقوانين براءة الاختراع أنّ برامج الحاسوب ولأنّها تستعمل للتعامل مع آلات الحاسوب وإدارتها ، فهي بذلك تصبح جزءا منها ولما كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الحاسب ، فهي من هذه الزاوية تصبح قابلة للبراءة[3].

---

[1] سعيدة بوزنون، المرجع السابق ،ص50.

[2] بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دارالخلدو نية للنشر والتوزيع، الجزائر، 2007، ط01 ، ص 37.

[3] بوعناد فاطمة زهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الاول لعام 2013، ص 66 .

نص الأمر رقم 03-07 الصادر في 2003[1] في المادة الثالثة منه على الشروط الواجب توافرها حتى يحظى الاختراع بالحماية بقولها: "يمكن أن تحمى بواسطة براءة الاختراع، الاختراعات الجديدة والناتجة عن نشاط اختراعي والقابلة للتطبيق الصناعي ...".

فالمشرع الجزائري استبعد صراحة المعطيات من مجال الحماية بواسطة براءات الاختراع[2] طبقا للمادة 07 من الأمر رقم 03 -07 التي تنص على " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب".

الفرع الثاني: خضوع معطيات الحاسب الآلي لنصوص الملكية الأدبية و الفنية

جاء الأمر رقم 03 -05 المتعلق بحق المؤلف والحقوق المجاورة[3] باستخلاص ما يلي: أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما المصنفات المعلوماتية.

الخاتمة:

وأخيرا وعلى ضوء ما تطرقنا إليه نستنتج أن الجريمة الناعمة أي الجريمة الالكترونية والتي هي نوع من أنواع الإجرام المعاصر تختلف عن باقي الجرائم المؤلوفة بالإضافة إلى صعوبة وضع تعريف جامع وموحد لها .

إضافة إلى أن المشرع الجزائري قام بمكافحتها بموجب تعديل قانون العقوبات رقم 15/04 ، فوضع العديد من النصوص القانونية التي تجرم الاعتداءات الماسة بالنظام المعالجة الآلية للمعطيات إلا انه لم يستحدث نصوص خاصة بالتزوير المعلوماتي وهو ما يعاب عليه.

[1] الأمر رقم 03-07 ،الصادر في 19 يوليو 2003 ،المتعلق ببراءات الاختراع، ج رالعدد 44.

[2] بوعناد فاطمة زهرة،المرجع نفسه،ص66.

[3] الأمر رقم 03-05 ،الصادر في 19 يوليو 2003 ،يتعلق بحقوق المؤلف والحقوق المجاورة ، ج ر العدد 4

المجرمون المعلوماتيون: خطر حقيقي يهدد عالم المعلوماتية

Information criminals: a real threat to the world of informatics

فيلالي أسماء دكتوراه في علوم التسيير
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
جامعة أبوبكر بلقايد – تلمسان- الجزائر-

مقدمة

منذ ظهور الحاسوب وتطور وسائل تكنولوجيا المعلومات والاتصال، بدأ الاعتماد الكلي عليها تدريجيا في كل مجالات الحياة، إلى أن أصبحت اليوم هي أساس التعاملات في المؤسسات وغيرها، وظهرت نتيجة ذلك عدة تسميات لهذا العصر منها: عصر المعلومات، العالم الرقمي أو ثورة المعلومات، ويعتبر هذا الأمر قفزة نوعية في مجال الأعمال، إذ أسهمت الوسائل الالكترونية في تسهيل التعاملات واختصار الجهد والوقت والتكاليف، إلا أن الاستعمال غير المشرع لها أدى إلى ظهور نوع جديد من الجرائم يسمى بالجرائم المعلوماتية، والتي تعتبر ظاهرة مستجدة ومستحدثة، ويطلق على مرتكبيها اسم المجرمين المعلوماتيين، إذ تعتبر هذه الفئة فئة مبهمة وغامضة سواء بالنسبة للضحية أو بالنسبة للقوانين والتشريعات التي تقف عاجزة في إيجاد قوانين موحدة للتعامل معها نظرا لصعوبة اكتشافها ومعرفة دوافعها وغاياتها.

يطلق على فئة المجرمين المعلوماتيين مصطلح "القراصنة المعلوماتيين"، وهو نوع جديد من المجرمين يختلف عن المجرمين التقليديين في العديد من الخصائص أولها مسرح الجريمة حيث تحدث الجرائم في عالم افتراضي غير ملموس، أين يختفي الجاني وراء شاشة وقد يبعد الجاني عن الضحية آلاف الأميال، وقد يكون أحدهما في بلد والآخر في بلد آخر حيث لكل بلد قوانينه الخاصة، وهذا ما يعقد الأمر فليس هناك نموذج موحد يصف الجريمة والمجرم المعلوماتي، إذ يمكن اعتبار فعل جريمة في بلد ما، في حين يعتبره بلد أخر أمر عادي، كما أن المجرم المعلوماتي له خصائص تميزه عن المجرم التقليدي أهمها الذكاء والمهارة والمعرفة التقنية، لكن وإن كان يتميز بصفات خاصة إلا أن هذا لا يغير حقيقة أنه مرتكب لفعل إجرامي يستوجب العقوبة، فالقوانين لا تحاسب على النوايا وإنما على النتائج.

لا شك أن المجرمين المعلوماتيين يختلفون في خصائصهم عن المجرمين التقليديين، كما أن دوافع الفئتين لارتكاب الفعل الاجرامي تختلف، وهذا ما يدفع بنا إلى طرح الاشكالية التالية :

ما هي أصناف المجرمين المعلوماتيين وما هي دوافعهم في ارتكاب الجرائم المعلوماتية ؟

للإجابة على هذه الاشكالية وجب الاجابة على التساؤلات التالية:

- من هو المجرم المعلوماتي؟
- ما هي خصائصه ؟ وفيما يختلف عن المجرم التقليدي؟
- ما هي أصناف مجرمي المعلوماتية؟
- ما هي دوافعهم في ارتكاب جرائمهم ؟

يتم الاجابة على الاشكالية والتساؤلات في ضوء فرضين أساسيين:

- المجرم المعلوماتي له نفس خصائص ودوافع المجرم التقليدي.
- المجرم المعلوماتي أقل خطرا من المجرم التقليدي.

تكمن أهمية هذه الدراسة في تطرقها لموضوع مستحدث يتناول نوع جديد من المجرمين ظهر نتيجة ظهور العالم الرقمي والاعتماد المطلق عليه في مختلف التعاملات اليومية، حيث تفصّل الدراسة في أنواع المجرمين المعلوماتيين وخصائصهم ودوافعهم لارتكاب الفعل الاجرامي.

ونحاول من خلال هذه الدراسة التوصل إلى الأهداف التالية :

- التعرف على أنواع المجرمين المعلوماتيين .
- معرفة سمات وخصائص شخصية المجرم المعلوماتي.
- ابراز أهم الدوافع التي تدفعهم لارتكاب الفعل الاجرامي.

تم الاعتماد في هذه الدراسة على المنهج الوصفي التحليلي، لوصف أنواع المجرمين المعلوماتيين، وتحليل شخصياتهم والدوافع التي تدفعهم لارتكاب الجرائم المعلوماتية.

لمعالجة اشكالية الدراسة تم تقسيم البحث إلى أربع محاور رئيسية :

المحور الأول: ماهية المجرم المعلوماتي

المحور الثاني: أصناف المجرم المعلوماتي

المحور الثالث: دوافع المجرم لمعلوماتي لارتكاب جرائمه.

المحور الرابع: كيفية الحد من الجريمة المعلوماتية.

المحور الأول: ماهية المجرم المعلوماتي

المجرم المعلوماتي يرتكب جرائمه بذكاء ومهارة دون الحاجة لاستخدام القوة والعنف، لذا يعتبر هذا النوع من الاجرام حديثا على الساحة القانونية، حيث اختلف المختصون في ايجاد قوانين موحدة للتعامل مع هذا النوع من الجرائم، لأن أنواع الجريمة المعلوماتية درجات، ولها ملابسات عديدة

لا يمكن حصرها، إذ يتطور الاجرام المعلوماتي بتطور التكنولوجيا، لذا ومن أجل التعامل الجيد والواضح مع هذا النوع من المجرمين يجب تحديد أولا ماذا تقصد بالجريمة المعلوماتية، وما هي الخصائص التي يتميز بها المجرم المعلوماتي.

1. تعريف الجريمة المعلوماتية.

الجريمة هي كل عمل محظور، ممنوع من قبل القانون، لهذا يجب أن تكون هناك قوانين من أجل تحديد الأفعال المسموحة والممنوعة، ومصطلح الجريمة المعلوماتية مفهوم غامض، موضوع له عدة مفاهيم وتفاسير، فالمجرم هنا مخفي وراء شاشة بعيدة، والجريمة تقع في عالم افتراضي غير ملموس، والضحية والجاني لم يلتقيا ولم يحصل بينهما تصادم، وقد يكون كل منهما في بلد مختلف، وعليه قد يرى البعض أن هناك صعوبة في تحديد أركان الجريمة، لذا لا يوجد إجماع على تعريف الجريمة المعلوماتية.

منظمة التعاون والتطوير الاقتصادي OCDE عرفت الجريمة المعلوماتية ك:" كل تصرف غير شرعي، غير أخلاقي أوغير مسموح، في انتقال و/أو المعالجة الآلية للمعطيات" هذا لا يخص فقط نشاطات الانترنت، وإنما كل ما يمكن فعله من خلال المعلوماتية، الاتصالات عن بعد، بما فيه الهواتف الثابتة أو النقالة، لكل التجهيزات التي تستخدم في المعالجة الالكترونية والمعلوماتية للمعطيات، أيضا كل عنصر وكل بنية تحتية تحكم في المعلومة الرقمية يمكن أن تكون معنية بالجريمة المعلوماتية.[1]

وتعتبر الجرائم المعلوماتية كل الجرائم التي ترتكب باستخدام الانترنت أو شبكة كمبيوتر أخرى، ويمكن أن تكون أجهزة الكمبيوتر متورطة في الجريمة بطرق مختلفة:[2]

- يمكن أن يكون الكمبيوتر أو الشبكة أداة الجريمة (تستخدم لارتكاب الجريمة).
- يمكن أن يكون الكمبيوتر أو الشبكة هدف الجريمة (الضحية).
- يمكن استخدام الكمبيوتر أو الشبكة لأغراض عرضية تتعلق بالجريمة.

[1] Solange Ghernaouti-Hélie, « **La Cybercriminalité-le visible et l'invisible**- », presses polytechniques et universitaires romandes, Lausanne, première édition, 2009, p 22.

[2] Michael Cross, " **Scene of the Cybercrime**", Second Edition, ed Syngress, 2008, p2.

يمكن الاصطلاح على مفهوم الجريمة المعلوماتية بالقرصنة المعلوماتية والتي عُرِّفت على أنها تطبيق تقني للقوة من أجل التأثير على أنظمة الاتصالات بمعنى أن القرصنة هي فقط مصطلح حديث للتصنت، اعتراض الاشارات، المراقبة وغيرها من التهديدات التقنية للخصوصية الالكترونية.[1]

وهناك من يرى أن القرصنة والجريمة المعلوماتية مفهومان مختلفان فليست كل قرصنة جريمة، ويختلف ذلك باختلاف دوافع الفاعل، ومن خلال تعريف المصطلحين نلاحظ أن بعض أو معظم أعمال القرصنة هي جريمة يعاقب عليها القانون، إلا أنه يوجد جانب مشرق، ويظهر ذلك من خلال تعريف Himanen و Wark اللذان اتفقا على تعريف القرصنة على أنها:

"القدرة على انشاء أشياء جديدة واجراء تعديلات واحداث اختلافات "فبالنسبة لهم الاختراق (القرصنة) يعني الاختلاف وامكانية دخول أشياء جديدة إلى العالم ليست بالضرورة جيدة المهم أنها جديدة.[2]

إلا أن Sherry Turkle وTaylor اعتبرا أن تعريف القرصنة على أنها تشير إلى كل شيء هو تعريف عام وعديم الفائدة لأن القرصنة مرتبطة بالتكنولوجيا وأعادا صياغة تعريف القرصنة كالتالي: "القرصنة هي ممارسة مادية تنتج اختلافا أو شيئا جديدا في الكمبيوتر، شبكة الأعمال والاتصالات."[3]

ولكن المتفق عليه أن القرصنة المعلوماتية هي نفسها الجريمة المعلوماتية باستثناء الأعمال التي يقوم بها المدافعون أو المختصون في تأمين أنظمة المعلومات على مستوى المؤسسات، حيث يكون الهدف من أعمالهم حماية أنظمة المنظمة والتصدي للمهاجمين، وبما أننا سنتطرق إلى جانب المدافعين وخصائصهم فسنعتمد خلال البحث على مصطلح القرصنة المعلوماتية.

2. تعريف المجرم المعلوماتي

يعتبر مصطلح المجرم المعلوماتي مصطلحا قانونيا، أما في عالم المعلوماتية فيتم استخدام مصطلح القراصنة المعلوماتيون أو المخترقون الذين ينقسمون إلى عدة أنواع مثل الهاكر والكراكر وأنواع أخرى سيتم ذكرها من خلال هذا البحث.

القراصنة هم أشخاص هدفهم الوصول إلى حواسب المؤسسة ودوافعهم مختلفة.

[1] Patrick Burkart, Tom McCourt ,” **Why Hackers Win-power and disruption in the network society**-”, University of California Press, Oakland , California, 2019, p5.

[2] Tim Jordan, “**Hacking – Digital Media and Society Series**-”, Polity Press, 2008, p7.

[3] Ibid, p10.

ويعرف القراصنة بصفة عامة ك:" أشخاص يصلون للأنظمة المعلوماتية بطريقة غير شرعية"[1] فالقراصنة هم أشخاص يقومون بأعمال غير شرعية وغير قانونية، لكن دون اللجوء إلى استخدام العنف، وإنما جرائمهم تكون بالاعتماد الكلي على الأنظمة المعلوماتية والتقنيات الحديثة التي أسفرت عنها الثورة المعلوماتية.

3. **خصائص المجرم المعلوماتي (القراصنة) :**

على الرغم أنه لا يمكن تصنيف جميع مجرمي المعلوماتية على أنهم أذكياء جدا أو جيدون أو سيئون إلا أنهم يشتركون في بعض الخصائص المشتركة، منها :

1.3 الفضول

الفضول الواسع والرغبة في تجربة الأشياء خارج الحدود هي من أهم خصائص المجرمين المعلوماتيين، إذ لا يخشون أن يصنعوا طريقتهم الخاصة، وعادة ما يكون قراصنة الكمبيوتر قراصنة حياة، حيث يقومون باختراق جميع الأشياء خارج أجهزة الكمبيوتر، إنهم أناس عندما يواجهون أمن المطارات يتحاورون بصمت كيف يمكنهم التسلل من أجهزة الكشف حتى لو لم تكن لديهم نية سيئة، انهم أناس يحاولون اكتشاف إذا كان بامكانهم تزوير تذاكر الحفلات المطبوعة باهظة الثمن بسهولة حتى لو لم تكن لديهم نية الحضور مجانا.[2]

2.3 المهارة

المهارة هي من بين أهم الصفات التي تجمع بين مجرمي المعلوماتية، وتميزهم عن المجرمين العاديين، إذ يتمتعون بقدر من الذكاء وإلمام جيد بالتقنية، واكتسابهم معارف علمية وعملية بحكم تخصصاتهم المرتبطة بالحاسوب في أغلب الأحيان[3]. إذ يتطلب تنفيذ الجريمة المعلوماتية قدرا من المهارة في المجال المعلوماتي ليس بالضرورة أن يكون عاليا وإنما قد تأتي المهارة بالممارسة.

3.3 المثابرة

---

[1] Jean-Paul Kurtz, « **Dictionnaire Etymologique, Lexicologique et Historique des Anglicismes et des Americanismes** », BoD- Books on Demand, 2013, p587.

[2] Roger A. Grimes, "Hacking the Hacker – Learn From The Experts Who Take Down Hackers-", John Wiley & Sons, Inc, 2017, p3

[3] محمد لينا جمال ، "الجرائم الالكترونية-ماهيتها و طرق مكافحتها-"، دار خالد الحياني للنشر و التوزيع، عمان ، 2016، ص 98.

إن المثابرة سمة أساسية في المجرم المعلوماتي، فكل مخترق يعرف جيدا عذاب الساعات الطويلة التي يحاول ويحاول فيها الحصول على مدخل لتنفيذ جريمته، إذ يبحث المجرم عن نقاط الضعف الدفاعية للنظام باستمرار، وخطأ واحد من قبل المدافع يجعل الدفاع بأكمله لا قيمة له، ويتشارك الجانبان في حرب مستمرة ينتصر فيها الأكثر إلحاحا ومثابرة.[1]

4.3 البساطة

يقوم المجرم المعلوماتي بأعمال تبدو خارقة لعوام الناس، لكن أفعاله في الحقيقة هي في غاية البساطة ولكنها مثيرة للاعجاب، وسبب الاثارة هو أن هذه الأفعال تكون دائما "ضد القواعد"، فالقيام بأشياء بسيطة وبارعة نادرا ما يكون سهلا وهذا هو تميز القراصنة[2]، ولكن البساطة لا تمنع وجود معرفة تقنية وجودة واتقان في التطبيق، فأعمال القراصنة يمكن التعبير عنها بجملة "السهل الممتنع".

5.3 جنس الذكور؟

ساد التفكير على أن مجرمي المعلوماتية عادة ما يكونون ذكورا، وأن مجال الاجرام المعلوماتي هو مجال ذكوري بحت، وهذا ما كانت تثبته الاحصائيات في البداية، لكن مع نهاية التسعينات أظهرت الاحصاءات أن الفجوة بين الجنسين أخذت في الاغلاق، وعلى الرغم أن نسبة الاجرام الصادر من جنس الاناث يبقى دائما منخفضا نسبة للذكور، إلا أنه لا يجب تجاهل المشتبه به على أساس الجنس، لأن علم الحاسوب لم يعد مهنة الذكور فقط، فقد أظهرت احصاءات وزارة التجارة الأمريكية أن 28.5% من المبرمجين هم من الاناث الآن، على الرغم من أنها نسبة مئوية صغيرة نسبة للذكور إلا أن هذا يعني أن الاناث أصبحت تمتلك الوسائل اللازمة لارتكاب الجرائم المعلوماتية أكثر من أي وقت مضى.[3]

6.3. الميل إلى التقليد

ويظهر ذلك في مجال الجريمة المعلوماتية لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه الأمر الذي يؤدي به إلى ارتكاب الجرائم.[4]

---

[1] Roger A. Grimes, op.cit, p4.

[2] Tim Jordan, op.cit, pp 10-11.

[3] Michael Cross, op.cit, p 88.

[4] غادة نصار، الارهاب والجريمة الالكترونية، العربي للنشر والتوزيع، 2017، ص46.

تعبر الخصائص المذكورة عن النقاط المشتركة بين جميع مجرمي المعلوماتية، إلا أن هناك خصائص أخرى خاصة بكل صنف منهم ويتم التفصيل في ذلك عند التطرق لأصناف مجرمي المعلوماتية.

المحور الثاني: أصناف المجرم المعلوماتي

لم يتفق الخبراء على تصنيف موحد لمجرمي المعلوماتية، فقد صنفهم Donn Parker (مختص في تحليل الجريمة المعلوماتية بمعهد Stannifére) إلى سبعة أصناف: الهواة، المهووسون، المحتالون، الجواسيس، المجرمون المحترفون، المحطمون، المتطرفون المثاليون. وصنفهم Didier Godart إلى خمسة أصناف: الهاكرز، الكراكرز، المحطمون، الجواسيس، المحتالون.

أما حسب النقيب Joël Riviére[1]: " هناك نوعين من مجرمي المعلوماتية: العبقري الصغير الذي يعرف الأنظمة كأصابعه ويعرف كيفية اكتشاف الثغرات، والهواة الذين لا يقومون سوى بتطبيق " وصفة المطبخ " التي قرؤوها أو سمعوها ."[2]

ومن خلال الاطلاع على عديد المراجع سنقوم بتصنيف المجرمين المعلوماتيين إلى سبعة أصناف: الهاكرز، الكراكرز، أطفال السيناريو، المستخدمين المستائين، المحتالين، الجواسيس، المناضلين.

1. الهاكرز Hackers

الهاكر ببساطة هو شخص يحب تعلم كيفية عمل كل الأشياء التي من حوله سواء الأشخاص، القوانين، المالية ،الالكترونيات، المعلوماتية وكل التكنولوجيات، شخص فضولي بطبيعته ويحب كثيرا ايجاد الحدود من أجل تجاوزها.[3]

ولكن التعريف السائد للهاكرز هو ذلك المتعلق بالشبكات والمعلوماتية، فالهاكرز هم قبل كل شيء "هواة الشبكات" يريدون فهم طريقة عمل أنظمة المعلومات واختبار في نفس الوقت قدرة الوسائل ومعارفهم، أغلب الهاكرز يؤكدون أن دخولهم للأنظمة كهواية للمعلوماتية وليس بهدف تدمير أوسرقة المعطيات.[4]

---

[1] Joël Riviére رئيس قسم تكنولوجيا المعلومات و الالكترونيات لمعهد البحوث الجنائية للدرك الوطني IRCGN و عضو في مجموعة عمل حول الجرائم المعلوماتية للانتربول.

[2] Franck Boulot &Didier Violle, « **La Guerre de l'information ou l'éloge de la paranoïa- plus de 500 faits réels pour apprendre à maitriser l'information-** », ed Publibook, 2005, p145.

[3] Simon Lévesque, « **le petit livre du hacker** », version 2013, sur le site web http://lpldh.pgon.ca, p7

[4] Jean-François Dhénin, « **Informatique Commerciale** », Ed Bréal, 2004, p72

وبالنسبة للخبراء فان الهاكر الحقيقي هو ذلك الذي يتسلل إلى الخادم من أجل اكتشاف ثغرات الحماية ويعلم بعد ذلك المسؤولين[1]

وكمثال على ذلك M.Raphael Gray بريطاني، 18 سنة حمل آلاف رموز بطاقات الأئتمان من عشرات المواقع، أراد فقط اثبات الثغرات الأمنية على هذه المواقع، أرسل هذه الرموز لقناة W.B.C، انزعج لعدم اظهار ردة فعل، فوضع هذه الرموز على الانترنت وكتب " كنت صادقا لكن تجاهلتموني، وضعت اذا المعلومات على الانترنت من أجل أن يعرف الجميع لأي درجة هذه المواقع ليست آمنة"[2]

هذه الفئة من القراصنة ذوي خبرة الكترونية، غالبا تتراوح أعمارهم بين 17 و25 سنة، يتابعون دروس معلوماتية ويقومون بأفعالهم من أجل المتعة الفكرية إذ يعتبرون القرصنة كلعبة، وهدفهم الأساسي هو اثبات قوتهم وقدرتهم على احباط الحمايات والسيطرة على الأنظمة المعلوماتية، الهاكر قادر على تصميم أنظمة قرصنة معقدة ومبتكرة، فهو خصم جد قوي، يقضي كل وقته حرا وكل لياليه في البحث عن ثغرات أنظمة الحماية، مشترك في كل قوائم المحادثات السرية للقراصنة ويمتلك كل برامج القرصنة التي يمكن الحصول عليها في الشبكات الموازية، عندما يأتي لقرصنة نظام معلوماتي يسبب عموما القليل من الخسائر، فهو يبحث فقط عن اثبات قدرته ونادرا ما يدمر المعطيات، ولكن هذا النوع من الأفعال يمكن أن يضر بصورة المؤسسة ويسبب خسائر.[3]

مشكلة هذه الفئة أنها غير واعية بأن أعمالها هي أعمال غير قانونية وغير شرعية وتتعامل مع الموضوع بدون جدية وباستهتار، ومن أفضل الأمثلة على ذلك Nick Whiteley الذي يعتبر كأشهر هاكر في المملكة المتحدة، Nick شاب ذو 19 سنة، جد هادئ، يعمل في الصناعة الكيميائية، كان شغوف بأنظمة ICL (International Computer Limited)، جمع كل المعلومات حولها، في البداية هاجم أنظمة ICL المتصلة على شبكة أكاديمية مثل المدارس والجامعات وبعدها بدأ باستكشاف كل أنظمة ICL الأخرى المتصلة بالشبكة الأكاديمية متنقلا من جامعة لأخرى، وبدأ من خلال حاسوبه ومن غرفته اختراق والتحكم في تثبيتات عدة مئات الآلاف أورو، كان يريد فقط تطبيق الجانب النظري الذي تعلمه، وكغيره من الهاكرز اعتبر

---

[1] Ibid, p72.

[2] Franck Boulot &Didier Violle, op.cit, p149.

[3] Jean-Marc Royer, « **Sécuriser l'informatique de l'entreprise-Enjeux, menaces, prévention et parades** », Ed ENI, France, 2004, p14

مغامرته بمثابة لعبة بينه وبين مديري النظام ،فبالنسبة له لا يمكن أن يكون هذا غير شرعي، بل هو فقط لعبة، ومن أجل إضافة بعض التوابل على اللعبة بدأ Nick يترك آثارا عند مروره، علامات لمديري النظام، يوقف أنظمة، يبعث رسائل، يبعث ملفات للطباعة، يمنع اتصال المدراء بالنظام، فأغضب مديري النظام وبدأ التحقيق حول ذلك، وإلى غاية لحظة توقيفه لم يفهم شيئا وظن أن هناك خطأ ما، وحتى وهو محاط بالمحققين لم يستطع الاقتناع أن ما فعله هو خارج القانون[1]

يعمل الهاكرز بصفة منعزلة وفردية أومن خلال مجموعات، ومن أشهر مجموعات الهاكرز :[2]

- **نادي الفوضى** « **Chaos Club** »: تأسس في ألمانيا سنة 1984، هدفه الرئيسي هو خلق الشقاق، بتبيان للسلطات أن الأمن المسؤولون عنه يمكن احباطه بسرعة.
- **فيلق العذاب** « **Legion of Doom** »: في 1984 أول عدد لجريدة متخصصة في القرصنة (Black Ice) خرج في الولايات المتحدة، هذا العدد تم تحضيره ونشره من طرف مجموعة من الهاكرز تسمى Legion of Doom، هذه المجموعة عموما تعتبر كنخبة القرصنة المعلوماتية، مثلها مثل "نادي الفوضى" هدفها الأساسي هو تشويش الشبكة الرقمية، المجموعة مهتمة أكثر بكشف عيوب وثغرات الأنظمة المعلوماتية من الجريمة.

2. الكراكرز Crackers

في حين يقوم الهاكرز بأعمالهم من أجل المرح، يقوم الكاركرز بأعمالهم من أجل متعة التدمير، فالكراكرز أكثر خطورة من الهاكرز، يستعملون ذكاءهم بطريقة شريرة، يبحثون عن الحاق الضرر وإظهار أنهم الأقوى، ويسعون دائما لإظهار وتأكيد تميزهم[3] تتراوح أعمارهم في الغالب بين 25 و45 سنة ولكن هذا ليس بقاعدة، ومن أبرز سمات وخصائص أفراد هذه الطائفة بأنهم ذوي مكانة في المجتمع، ومتخصصين في مجال التقنية الالكترونية[4]

---

[1] Didier Godart, « **Sécurité Informatique – risques ,stratégies et solutions** », Ed des CCI de Wallonie SA, Deuxième édition, 2005, pp 25-27.

[2] Ibid, p26

[3] Bureau conseil de la direction centrale de la sécurité des systèmes d'information «**Menaces sur les systèmes informatique « Guide N 65** »»», paris, version du 12 septembre 2006, p8

[4] محمد دباس الحميد، ماركو ابراهيم نينو، "**حماية أنظمة المعلومات**"، دار الحامد للنشر و التوزيع، الطبعة الأولى، 2007، ص73

يستغلون الثغرات الموجودة في إجراءات الوصول للأنظمة المعلوماتية، يحاولون الوصول إلى أهداف معينة دون تحقيق أرباح، فقط من أجل المتعة، يسعون دائما لكسر أنظمة الحماية، غالبا ما يكونون مهنيين، دوافعهم غير واضحة ومفهومة، يطلق عليهم عدة أسماء أخرى منها: المفرقعين، المحطمين، مجرمي المعلوماتية.

تقوم أعمالهم على زرع الفيروسات والبرامج الخبيثة من أجل تدمير أكبر نسبة من الحواسب والأنظمة، فمثلا في 2 ماي 2000، إعصار عالمي انتشر من الفلبين في شكل بريد جذاب " **أحبكم**" يحث على فتح ملف مرافق، الرسالة تتضمن فيروس وتحديدا عبارة عن دودة مهمتها الأساسية هي إعادة إرسال الرسالة الأصلية إلى كل دفتر عناوين المستلم، مستغلة ثغرة في outlook أصابت 3 ملايين حاسب في 4 أيام فقط، وهذا ما سمح بتحديث أنظمة الرسائل قبل بداية اليوم.[1]

وفي سبتمبر 2017 مشتركي Netflix استقبلوا رسالة احتيال تدعوهم لتحديث معلوماتهم البنكية والاّ يتم إلغاء اشتراكهم[2]، و بالتالي يقوم المهاجمون بتجميع المعلومات لاستغلالها في هجماتهم.

كما أنهم يعتمدون في تنفيذ جرائمهم على هجمة رفض الخدمة وخصوصا فيروس bot، هذا الفيروس لا يعمل سوى أنه ينتشر، ولكن في ساعة محددة أو إشارة معطاة آلاف أو ملايين الآلات المصابة تتصل بنفس الخادم المستهدف وتثير انهياره.[3] كما يطلق عليه اسم شبكة الروبوتات أوالبوت نت (botnets) ويتمثل خطرها في سيطرة شخص أو مجموعة يعرف بالمتحكم (Master)، على شبكات ضخمة من الأجهزة الحاسوبية ربما يبلغ عددها الآلاف بل حتى الملايين، ويمكن لذلك المتحكم أن يطلب من تلك الأجهزة القيام في توقيت محدد عن طريق برنامج تحكم يطلق عليه برنامج السيطرة والتحكم بتنفيذ أوامر معينة لأغراض تجارية أو تخريبية، وتتم كل هذه الأمور بشكل خفي ومن الصعب جدا اكتشافها من مستخدمي الأجهزة.[4]

[1] Pierre-Luc REFALO, «**la sécurité numérique de l'entreprise«l'effet papillon du hacker»**», Groupe EYROLLES, Paris, 2013, p43.

[2] Lionel Roux, Cybercriminalité : exemples et mesures pour protéger les projets sensibles, 2018, voir : www.appvizer.fr visité le 17/05/2020 à : 12 :00.

[3] André Vaucamps, CISCO: «**Sécurité des routeurs et contrôles du trafic réseau**»,Ed ENI, 2010, p14.

[4] مأمون العزب ،"**أمن المعلومات في فضاءات انترنت الأشياء**"، مجلة التقدم العلمي، العدد 99، مؤسسة الكويت للتقدم العلمي، أكتوبر 2018، ص 14.

ومن أشهر التهديدات التي خلقتها هذه الفئة كان سنة 2011، ففي سنة 2010 أصبح مؤسس ويكيليكس "جوليان اسانج" شخصية مجلة التايم لتلك السنة بعد نشر آلاف من الوثائق الحساسة سياسيا والتي أحرجت واشنطن والحكومات الأخرى في العالم، وفي سنة 2011 كانت الجهود التي بذلتها العديد من الحكومات لاسكاته واسكات ويكيليكس قد جعلته أول شهيد في العالم الفضائي، واستجابة لذلك هاجم جيش من الفوضويين المعلوماتيين الذين يعملون باسم « Anonymous » هذه الحكومات، وكذلك هجمات رفض الخدمة على شركات الخدمات المالية « Paypal »و « Mastr Card » بعد قطع روابطها مع ويكيليكس، كما عانت « Sony » هجمات على المعلومات الشخصية التي تتضمن عشرات ملايين الزبائن، كما استهدفوا اتصالات حوالي 300 شركة كبيرة في هجمة واحدة على « Nasdaq » التي هي إحدى أكبر البورصات في العالم.[1]

حرية البرامج، حقوق النشر، بطاقات الائتمان هي اهتمامهم، ففي أوائل سنة 2000 تم تسجيل عدة حالات لسرقة أرقام بطاقات الائتمان مثل حالة Curador et Maxus حيث قام مراهقان ذو 18 سنة بنشر 26000 رقم بطاقة ائتمان من خلال 8 مواقع في أمريكا، كندا، تايلندا، اليابان، انجلترا، وعند توقيف هؤلاء الكراكرز صرحوا أنهم استغلوا ثغرة جد معروفة لبرنامج Microsoft المركب على خوادم الويب للمحلات الافتراضية من أجل أن يتمكنوا من الوصول لقواعد البيانات لضحاياهم وتحميل المعلومات الحساسة، وفي فيفري 2003 تم الوصول من الخارج لحواسب[2] DPI، وكان الصيد بليغا، حوالي 13 مليون رقم بطاقة ائتمان، وهي أكبر سرقة لأرقام بطاقات الائتمان، هذه الحادثة لم تتسبب في خسائر مالية لأصحاب البطاقات، وإنما فقط ايقاف تشغيل البطاقات، وهذا بالنسبة للمؤسسات الكبرى خسارة كبيرة في السمعة والصورة. إلى جانب سرقة المعلومات الحساسة، الكراكرز يهاجمون أيضا عن طريق نقل وبيع بطريقة غير شرعية البرامج، الموسيقى والأفلام.[3]

من أشهر الكراكرز في العالم هو الأمريكي Kevin Mitnick واختلف حول تصنيفه هاكر أو كراكر، لكن من خلال الأعمال التي قام بها فقد تم تصنيفه ككراكر، حيث اشتهر من خلال

---

[1] آيان بريمر ترجمة فاطمة الذهبي، عالم بلا قيادة- كل أمة لنفسها الرابحون والخاسرون في عالم المجموعة الصفرية، دار الفارابي، 2014، ص125.

[2] DPI: مؤسسة مهمة معنية بمعالجة المعاملات عن طريق بطاقات الائتمان لصالح المشترين

[3] Didier Godart, op.cit, pp 29-30.

تنفيذه عدة أنشطة منها كسر حماية نظام أمن الكمبيوتر الحكومي الأمريكي، كما استخدم تقنية خداع HP (IP-Spoofing) من أجل اقتحام شركات: فوجيستو، موتورولا، نوكيا وآخرين بحثا عن برامج للهواتف المحمولة لمحاولة تأمين أنظمته الخاصة[1] كما اتهم بسرقة ملايين الدولارات في البرامج، اقتحم دون موافقة خادم "البنتاغون" وامتلك وسرق رموز الدخول وكلمات المرور، اعترض اتصالات الكترونية، وفي ظل مطاردة افتراضية طويلة، تم القبض عليه وأصبح يعتبر كرمز عالمي بالنسبة لمجتمع كامل من مستخدمي الانترنت.[2] بعد كل هذا أصبح Kevin مستشارا لأمن الكمبيوتر وقضى وقتا طويلا يساعد الصالح العام.

3. أطفال السيناريو Script Kiddies

هم قراصنة مبتدئين، غالبا ما يكونون في عمر المراهقة، ليس لديهم مهارات، يقتحمون الأنظمة بعد قراءة بعض الوثائق عن أمن المعلومات سواء في الكتب أو الانترنت، لا يعملون سوى على إعادة استعمال رموز أو برامج جاهزة للاستخدام دون أي معرفة أوفهم لها [3] لكن رغم جهلهم في مادة المعلوماتية والأمن إلا أنهم يمثلون تهديد جد مهم، فالخطر يأتي من إمكانية حصولهم على برامج قرصنة مصممة من قبل قراصنة خبراء، تكون هذه البرامج سهلة الاستعمال، يكفي الاشارة لعنوان موقع الويب المراد الهجوم عليه، يحاولون بصفة مستمرة ومستقلة تنفيذ عدة هجمات ضد الموقع مستهدفين ثغرات البرامج المعروفة، فإذا وجد البرنامج ثغرة يمنح الوصول للمخترق الهاوي الذي سيفعل ما يريد.[4] سموا بهذا الاسم انطلاقا من قلة مهاراتهم وخبراتهم واعتمادهم على سيناريو مكتوب يطبقونه بحذافيره دون ذكاء وابداع وإنما يحتاجون القليل من المعرفة التقنية.

4. المستخدمين المستاءين

في العديد من الحالات، أفعال الاجرام المعلوماتي يصدر من مستقدمين قدامى، غالبا يكونون عمال في الخدمات المعلوماتية، تركوا المؤسسة في حالة سيئة ويريدون الانتقام، كانوا جزءا من المؤسسة، يعرفون هندسة المعلوماتية ما يسهل لهم الهجوم، لديهم عدة كلمات مرور يمكن أن

---

[1] Tim Jordan, op.cit, p1.

[2] Franck Boulot &Didier Violle, op.cit, p146

[3] ACISSI, «**Sécurité Informatique – Ethical Hacking: Apprendre l'attaque pour mieux se défendre**-», Ed ENI, 2009, p17.

[4] Jean-Marc Royer, op.cit, pp 14-15.

تكون قد غيرت بعضها ولكن البعض تكون لا تزال مفعلة يمكن سهوا من المؤسسة أو أنهم ليس لديهم علم بمعرفته لها.[1]

يطلق على هذه الفئة أيضا المنتقمون، لأن صفة الانتقام والثأر هي ما تميز به، هذه الفئة لا تتفاخر بأعمالها كبعض الفئات، بل تقوم باخفاء وانكار كل ما ينسب اليها من تهم.

5. المحتالين

هذا النوع من المجرمين يحكمه طمعه، ويتميز بالحذر والسرعة والفعالية، يقتنص فرص المبادرة، يعرف متى، أين وكيف ينفذ هجومه[2] يشبه كثيرا المجرمين التقليديين لأن هدفه الحصول على المال بأي طريقة: سرقة، تزوير، اختلاس...لذا غالبا ما تكون وجهتهم المؤسسات المالية كالبنوك، مؤسسات التأمين.

ولكن المعلوماتية سمحت لهم بتنفيذ أعمالهم دون أخطار حقيقية، مع احتمالية الأرباح الكبيرة، وأكبر دليل على ذلك حادثة تواصل المافيا بطريقة غير مباشرة بخبير معلوماتي في مؤسسة خدمية من أجل أن يضع لهم نظام تعويضات بين البنوك (المقاصة بين البنوك) على شبكة Swift المستخدم من قبل حوالي 1700 بنك في 54 دولة، المافيا أرادت تحمّل تكاليف تطوير البرنامج مع ضمان امكانية مراقبة وجمع بطريقة غير شرعية جزء من التدفقات المالية العابرة عبر الشبكة، لكن لحسن الحظ لم تنجح العملية.[3]

وبالتالي هم عبارة عن مجرمين تقليديين أو بالأحرى لصوص ومافيا استعملوا التكنولوجيا كوسيلة لارتكاب جرائمهم من أجل تخفيض نسبة الخطر.

6. الجواسيس

يشاركون في الحرب الاقتصادية، يعملون لحساب دولة أو لحساب منافس، صبورين ومحفزين، يتقنون الحفاظ على سر نجاحهم من أجل عدم إثارة الشكوك وإتمام أعمالهم في الظل، يتحركون غالبا من داخل المؤسسة، إما عن طريق ايجاد وسيلة للاختراق، أو بشراء شخص لديه صلاحية الوصول إلى الأجهزة، هدفهم سرقة المعلومات أو القضاء على المعطيات الاستراتيجية للمؤسسة،

[1] Ibid, p15.

[2] Robert Longeon ,Jean-luc Archimbaud, «**guide de la sécurité des systèmes d'information à l'usage des directeurs**», Centre National de la Recherche Scientifique(CNRS), Paris, 1999, p12.

[3] Liang Jiansheng, «**Criminalité informatique**», Rapport de stage en service de documentation générale du secrétariat générale d'interpol, Enssib, 1999, p28.

في كل الأحوال الجواسيس لديهم مستوى هائل في التحكم بالذات، إضافة إلى قدرة كبيرة في التأقلم مع المحيط.[1]

هذا النوع من المجرمين أو القراصنة كان يقوم بأعمالها سابقا عن طريق عمله في مؤسسة ما لحساب مؤسسة منافسة من أجل نقل الأخبار وسرقة المعلومات الحساسة، لكن التطور التكنولوجي والحواسب سهلت مهمته، فأصبح يقوم بكل أعمال الجوسسة دون الاقتراب من المؤسسة المستهدفة.

7. **المناضلين**

هذا النوع من القراصنة هم الأكثر خطورة، لديهم قضية ما يدافعون عنها، وعادة ما يقومون بإرسال رسائل التهديد وتدمير البيانات المخزنة لمجرد أن يسجلوا وجهة نظرهم، لا يعملون داخل حدود الدولة، بل يمكن أن يعمل من أي مكان في العالم مما يصعب عملية اقتناصهم[2]، لا يسعون لتحقيق أهداف شخصية أومكاسب مالية بل يحاولون الإضرار بكل من يخالف معتقداتهم ويعارض مذاهبهم كما يحاولون ضم أكبر عدد إلى صفوفهم لديهم قدرات مالية هائلة وشبكة علاقات عالمية تمكنهم من ارتكاب مختلف أنواع الهجوم في مختلف الأماكن، كما يسعون إلى تحقيق نتائج خارقة من أجل إحداث ضجّة عالمية وإحداث الحرب السيكولوجية، وتخويف الناس.

هذا التصنيف لمجرمي المعلوماتية هو تصنيف مفصل، لكن هناك من قسم مجرمي المعلوماتية أو القراصنة إلى 3 أنواع: القبعات البيضاء، القبعات الرمادية والقبعات السوداء.

1. **القبعات البيضاء White Hats**

هم هاكر جيدون لا يقومون بنشاطات غير قانونية وغير أخلاقية، عند اكتشاف الثغرات يعمل القبعات البيضاء على نشر اكتشافاتهم واعلام المسؤولين بذلك، وأحيانا نجدهم أشخاص مدافعين يعملون على حماية الأنظمة.

2. **القبعات الرمادية Grey Hats**

القبعات الرمادية هي هجينة انطلاقا من القبعات البيضاء والقبعات السوداء ، هم عبارة عن هاكر كفئ، يتصرف مرة بروح القبعات البيضاء ومرة بروح القبعات السوداء، نيتهم ليست

[1] Menaces sur les systèmes informatique «Guide N 65», op cit, p9

[2] دياب موسى البداينة، "الجرائم الالكترونية: المفهوم و الأسباب"، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات و التحولات الاقليمية و الدولية، عمان، الأردن، 2014، ص 21.

سيئة ولكن يرتكبون أحيانا جرائم، وفي الحقيقة العديد من الهاكر يقولون أنهم قبعات بيضاء ولكن في الحقيقة يظهرون أنهم قبعات رمادية لأنهم في كثير من الأحيان لا يظهرون اكتشافاتهم ويستغلونها لفائدتهم.[1] وهناك من يعتبر القبعات الرمادية هي قبعات سوداء فإما أن تفعل أشياء غير قانونية أولا.

3. القبعات السوداء Black Hats

هم المخترقين الذين يشاركون بسهولة في الأنشطة غير القانونية وغير الأخلاقية، ويخفون اكتشافاتهم من أجل استغلالها لصالحهم، ولكن يمكن للقبعات السوداء أن تصبح بيضاء، وهذا كثيرا ما يحدث ولكن المهم يجب أن يحدث هذا قبل أن يضطروا لقضاء وقت طويل في السجن، ومن أشهر الأمثلة على ذلك Kevin Mitnick الذي بعد أن كان كراكر معروف، عاش بعد ذلك وقضى وقتا طويلا كمساعد يساعد الصالح العام [2]

- **بين المهاجم والمدافع**

إذا قمنا بمقارنة فكرية بين المهاجم والمدافع، فان المدافعين في المتوسط يكونون أكثر ذكاء من المهاجمين، لأن المدافع يعرف كل شيء يقوم به المجرم المعلوماتي، بالإضافة إلى كيفية ايقاف الهجوم، يعمل خلف الكواليس بصمت ومثالية طوال الوقت، فأغلب المجرمين المعلوماتيين -ما عدا فئات معينة- متوسطو الذكاء، يكررون فقط شيئا نجح لمدة 20سنة، وعليه فان الأشخاص الأذكياء في عالم الكمبيوتر ليسوا المهاجمين بل المدافعين، إذ عليهم أن يعرفوا كل ما يعرفه المخترق وأن يخمنوا ما قد يفعله في المستقبل وأن يبنوا دفاعا سهل الاستخدام وبجهد منخفض ضد كل شيء.[3]

المحور الثالث: دوافع المجرم المعلوماتي

لكل نوع من أنواع مجرمي المعلوماتية السابق ذكرهم دافع يدفعه لارتكاب جريمته بغض النظر عنه إذا كان يعتبرها جريمة أم لا، فالهاكرز دافعهم التسلية والابداع واثبات الذات، والكراكرز دافعهم متعة التحطيم والتدمير، أطفال السيناريو دافعهم الرغبة في تطبيق النظري الذي اكتسبوه، المستخدمين السابقين دافعهم الانتقام، المحتالين دافعهم الربح المالي، الجواسيس دافعهم التجسس الصناعي، المناضلين دافعهم اثبات وفرض آراءهم، ولكن لا يمكن الجزم بأن لكل

---

[1] ACISSI, op.cit, pp 16-17.

[2] Roger A. Grimes, op.cit, p5.

[3] Ibid, p3, p6.

صنف دافع واحد ومعين، لأنه أحيانا يدفع المجرم مجموعة من الدوافع مجتمعة، لذا سنعرض الدوافع التي تسببت في أغلب الجرائم المعلوماتية وأكثرها تسببا وتكرار، بغض النظر عن خصائص مرتكبها .

1. الربح المالي

الربح المالي يمكن أن يكون الدافع الأكبر حصة من مجموع دوافع ارتكاب الجرائم الالكترونية نظرا للفائدة التي يعود بها على الجهة المنفذة، سواء باختراق أنظمة المؤسسات وخاصة المالية منها وسرقة ما يمكن سرقته، وإما بالتسبب في خسائر للضحية مما يعود بالنفع على الجهة المهاجمة كحصة سوق أو عروض تجارية أو إفقاده مصداقيته، غالبا ما يتم مهاجمة مؤسسات مالية، ولكن من الأسهل مهاجمة مؤسسات أقل حماية مثلا:[1]

- مؤسسة تنظم مسابقة بهدايا، بقرصنة خوادمها المعلوماتية التي تضم قوائم الرابحين، يمكن للمجرم إضافة اسمه على رأس القائمة.
- مؤسسة تبيع منتجات على الانترنت، بالدخول غير الشرعي للحواسب، يمكن بعث المنتجات مجانا أو تحميل أرقام بطاقات ائتمان بعض الزبائن واستغلالها.

ومن أجل توضيح مدى وقدر الأرباح المحققة عند النجاح في ارتكاب الجريمة الالكترونية يقول أحد المجرمين المحترفين في سجن كاليفورنيا: "لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية، وبإمكاني أن أكرر ذلك في أي وقت، لقد كان شيئا سهلا فأنا أعرف أسلوب عمل جهاز حاسوب الضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني "[2]

كما يمكن ادراج تحت الدافع المالي ما تقوم به بعض الشركات المتخصصة بإنتاج الحلول الأمنية للمؤسسات حيث تقوم بإطلاق هجمات إلكترونية على شكل برمجيات خبيثة عبر الشبكة بشكل سري وتقوم بعد ذلك بإعلان أنها قامت بإنتاج مكافح أو معطل قادر على حماية النظام من هذه

---

[1] Jean-Marc Royer, op.cit, p 13.

[2] نهلا عبد القادر المومني، "**الجرائم المعلوماتية**"، دار الثقافة للنشر و التوزيع، الطبعة الاولى، عمان، 2008، ص91
عن: صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولود معمري تيزي وزو ـ 2013، ص 39.

البرمجيات فتهافت الشركات والمؤسسات لشراء ذلك المكانح مما يعود بالنفع على الشركة المنتجة بالربح.[1]

وتعتبر الجرائم من هذا النوع الأكثر انتشارا، وسنورد مجموعة من الأمثلة عن الجرائم بدافع مالي:

- 1994 Vladimir Levin شاب روسي ذو33 سنة، يقضي أيامه في تطوير البرامج بدون مصلحة حقيقية، إلى أن اكتشف في يوم ما أن كل الأنظمة المعلوماتية لها ثغرات بما فيها البنوك، بالنسبة له هذه الأبواب المفتوحة هي بمثابة دعوات، وبمساعدة بعض المتواطئين فتح Vladimir حسابات بنكية تحت هويات خاطئة في أروبا، أروبا الشرقية وبلدان أخرى، دخل إلى نظام معلومات CitiBank في الولايات المتحدة الأمريكية من أجل سرقة قائمة أسماء المستخدمين وكلمات المرور من أجل تحويل أموال، المبلغ الاجمالي قدر ب 10 ملايين دولار، تم توقيفه سنة 1995 وحكم عليه بالسجن 3 سنوات ويعتبر كأول سارق معلوماتي لبنك، استرجعت CitiBank 400 ألف دولار.[2]
- وفي نوفمبر 2017 ما يقارب 60 مليون من حسابات مستخدمي ومديري "Uber" تمت قرصنتها، المؤسسة الأمريكية قدمت 100000دولار للقراصنة مقابل اتلاف المعلومات المجمعة وصمتهم لكن لا شيء يمكن أن يضمن ذلك.[3]
- قام ثلاث أشخاص: Albert , Alexander Suvorov , Maxim Yestremsky Gonzalez بقرصنة نظام معلومات سلسلة مطاعم أمريكية عن طريق سرقة المعطيات وبطاقات الائتمان، القراصنة دخلوا إلى نظام معلومات 11 مطعم للسلسلة الشعبية Dave and Buster's وأعادوا بيع معطيات 5000 بطاقة متسببين في خسارة 600 ألف دولار أمريكي بالنسبة للمنظمات المرسلة لبطاقات الائتمان، تم توقيف Maxim من طرف السلطات التركية أما Alexander تم توقيفه من طرف السلطات الألمانية بطلب من واشنطن.[4]

---

[1] أسامة سمير حسين،"**الاحتيال الالكتروني- الأسباب و الحلول** - "، الجنادرية للنشر و التوزيع، الطبعة الأولى،2011، ص 97.

[2] Didier Godart, op.cit, p35.

[3] Lionel Roux, op.cit.

[4] Solange Ghernaouti-Hélie, op.cit, p27

- تمكن بعض القراصنة من اختراق مجموعة "سيتي جروب" الأمريكية 2009، وسرقة عشرات الملايين من الدولارات، مما أصاب النظام الاقتصادي الأمريكي بخسائر فادحة، هذا الفعل تبين بعد ذلك أنه تم بالتنسيق بين مجموعة من القراصنة الأمريكيين وعصابة روسية من خلال شبكة الانترنت.[1]
- قام أحد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط.[2]

وفي الآونة الأخيرة ظهرت و انتشرت هجمة تعرف بهجمة الفدية، وهي عبارة عن رمز خبيث يمنع الضحية من الوصول إلى محتوى ملفاته من أجل ابتزازه بالأموال، وتعتبر أخطر هجمة يتم استخدامها مؤخرا، و من أشهر الاحتيالات التي تمت بالاعتماد على هذه الهجمة:[3]

- 19 مارس 2019 المؤسسة النرويجية المتخصصة في صناعة الألمنيوم Norsk Hydro تعرضت لتوقف جزء كبير من شبكتها وبدأت بتحقيق انتاجها يدويا بعد اصابتها بهجمة الفدية .« Loker Goge » ، بامتلاكها نسخ احتياطية لمعطياتها قررت عدم دفع الفدية، لكن انخفاض انتاجيتها عقب الأزمة كلف 40 مليون دولار.
- 7 ماي 2019 مدينة « Baltimore » كانت ضحية هجمة فدية « Robin Hood » التي تسببت في عدم اتاحة العديد من الخدمات خاصة خدمة الرسائل المهنية للبلدية، الخطوط الهاتفية والبنية التحتية للدفع عبر الانترنت، وطلب المجرمون فدية 100000 دولار مع زيادة 10000 دولار عن كل يوم تأخير.
- في ديسمبر2019 مجموعة مجرمين أعلنوا تعرضهم للمؤسسة الامريكية « southwire » بهجمة الفدية « Maze » وفي ظل تجاهل وصمت المؤسسة عن الاعلان، سرعان ما نشر المهاجمون بعض الوثائق الداخلية على موقع انترنت متاح، فرفعت المؤسسة دعوى قضائية ضد الموقع وتم اغلاقه، وردا على ذلك وفي جانفي 2020 قاموا بنشر 14 Gb من معطيات نظام معلومات « southwire » على منتدى مهاجمين « russophone ».

---

[1] ايهاب خليفة، "القوة الالكترونية – كيف يمكن أن تدير الدول شؤونها في عصر الانترنت-"، المنهل، 2017، ص 227.

[2] محمد لينا جما ، مرجع سابق، ص106.

[3] TLP : WHITE, Etat de la menace Rançàngiciel « à l'encontre des entreprises et institutions », ANSSI , 05/02/2020 pp 10-11, voir : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

فدافع المال هو أكثر دافع يجمع بين المجرم التقليدي والمجرم المعلوماتي، حيث أن أغلب دوافع الاجرام التقليدي هو الحصول على المال، لذا قد يكون أغلب المجرمين المعلوماتيين الذين يتحركون بدافع المال والذي يطلق عليهم "المحتالين" هم مجرمين تقليديين استغلوا العالم الافتراضي لارتكاب جرائمهم بأقل خطورة، وعليه فان أنظمة المعلومات هنا هي وسيلة وليست هدفا.

2. التجسس الصناعي

دافع التجسس الصناعي يكون على مستوى الدول والمؤسسات الكبرى، وغالبا ما يكون الدافع الحقيقي من التجسس هو المنافسة، التي تكون هنا بطريقة غير شرعية، حيث يبحث المخترقين هنا عن المعلومات الحساسة الخاصة بالشركة المنافسة أو الدولة المستهدفة، دون سرقة أموال أو تخريب أنظمة.

إذ يمكن اختراق شبكة المعلومات الخاصة بالشركة المستهدفة لمعرفة ميزانيتها وعدد موظفيها ومراحل إعداد المنتج وبراءات الاختراع التي حصلت عليها وأسرار تطوير صناعتها وقواعد بيانات عملائها وخططها التسويقية من دون عناء أو مخاطرة، وقد تمر سنوات دون أن تدرك الشركة المستهدفة أنها ضحية عملية اختراق.[1]

مؤسسة Ruag المؤسسة السويسرية للأسلحة وأنظمة الدفاع، تعرضت لهجمة الكترونية، وكانت مخترقة من قراصنة لعدة شهور، حيث سمحت هذه الهجمة ضد Ruag للمخترقين بالوصول إلى عشرات الآلاف من المعلومات الحساسة، فبعد تغلغلهم داخل الشبكة قاموا بتنفيذ نشاط جانبي عن طريق اصابة أجهزة أخرى والحصول على امتيازات عالية، واحدة من أهم أهدافهم كان "دليل الأنشطة" الذي يسمح لهم بمراقبة أجهزة أخرى والوصول إلى المعطيات التي تهمهم، وقاموا باستخدام HTTP من أجل تحويل المعطيات إلى الخارج.[2]

وتعاني الولايات المتحدة من اختراق شبكات الشركات الأمريكية بهدف سرقة المعلومات التجارية، وبراءات الاختراع وأسرار التكنولوجيا المتقدمة من شبكات وأجهزة الشركات العاملة في هذا المجال، وقد نشرت مجلة التايم تقريرا حول تعرض كبريات شركات الصناعة الأمريكية لسلسلة من الهجمات الالكترونية مصدرها الصين، وأكد تقرير "مانديات" – إحدى شركات الأمن الالكتروني الأمريكية- لعام 2013 أن الصين قد هاجمت على الأقل 141 مؤسسة

[1] نفس المرجع، ص220.

[2] Marie de Fréminville,«**La Cybersécurité et les décideurs-sécurité des données et confiance numérique**-», ISTE Editions Ltd, 2019, pp 22-23.

صناعية أمريكية في بداية 2006 وترتبت عليها سرقة بيانات وبراءات اختراع وحقوق ملكية فكرية ونتائج أبحاث وقواعد بيانات عملاء.[1]

وفي ديسمبر 2009، أوردت الحكومة الكورية الجنوبية تقريرا عن تعرضها لهجوم نفذه قراصنة كوريين شماليين بهدف سرقة خطط دفاعية سرية تتضمن معلومات عن شكل التحرك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية.[2]

وفي جويلية 2010، أعلنت ألمانيا أنها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد. [3]

وعليه بدأت تُرسم جغرافيا سياسية جديدة تضع في موضع القوة البلدان التي تحكم في هذا السلاح وتجبر الآخرين على الدفع من أجل حماية المصالح الوطنية، وظهور وسائل التجسس الفعالة جعلت هذا المفهوم قابل للتحقيق، شبكة " Echelon " تمثل أحسن مثال على ذلك.[4]

3. التحدي التكنولوجي والابداع

إن التكنولوجيا تثبت فشلها في العديد من الأحيان، ويعبر عن هذا ب"حتمية التكنولوجيا"، والقراصنة هم المحاربون لهذه الحتمية التكنولوجية واصلاح التقنيات حتى تكون هناك قرارات جديدة، فاذا كان هناك مجموعة من الهاكرز تكاتف لانشاء برنامج قوي لمعالجة الكلمات أو متصفح ويب أنظف وأسرع فانهم يعيدون بناء أشكال الحتمية التكنولوجية التي سيعمل من خلالها أولئك الذين يستخدمون حزم البرامج هذه، وإذا كتب مخترق ذو دوافع سياسية حزمة برمجيات تخفي البيانات حتى يتمكن نشطاء حقوق الانسان من تمرير المعلومات بأمان فان هذا المخترق يتحدى قدرة التقنيات التي تحددها الدولة على التجسس على الناشطين، وعليه فان القراصنة هم محاربوا الحتمية التكنولوجية، إذ يساهمون في ابتكار طرق جديدة لعمل التكنولوجيا من خلال الانخراط في التحديات اليومية للتكنولوجيا.[5]

Linus Torvalds هاكر، اشتهر بقيادته تطوير نظام تشغيل يسمى Linux، بدأت حزمة البرامج المعقدة هذه كتمرين تقني ل Torvalds الذي كتب وأطلق المكون الأساسي (النواة)

---

[1] ايهاب خليفة، مرجع سابق، ص220، ص222.

[2] فيصل محمد عبد الغفار، "**الحرب الالكترونية** "، الجنادرية للنشر و التوزيع، 2016، ص13.

[3] نفس المرجع، ص13.

[4] Abbas Jaber, «les infractions commise sur internet», L'Harmattan, Paris, 2009, p37.

[5] Tim Jordan, op.cit, p14

لنظام العمليات، وبعدها أشرف Torvalds على جهد جماعي موسع لكتابة المزيد والمزيد من مكوناته، حتى ظهر Linux كنظام تشغيل حر ومتطور يعتبره الكثيرون منافسا تقنيا مهما لنظام تشغيل Microsoft Windows، وحسب Torvalds فان أهم دوافع الهاكر هي الابداع.[1]

وحسب Himanen "فان القيمة الأعلى والمحددة لأخلاقيات عمل القراصنة هي "الابداع"، أي الاستخدام التخيلي لقدارت المرء والتجاوز المستمر المدهش لنفسه وإعطاء العالم مساهمة قيمة حقا" وبالنسبة ل Wark "فان الاختراق يعني الاختلاف، إذ يخلق القراصنة امكانية دخول جديدة للعالم".[2]

هناك هجمات تشن فقط لإثبات أن أنظمة الحماية المتخذة ضعيفة ويمكن اختراقها، فقد قامت عصابة هاكرز متكونة من 5 أشخاص :4 مصريين وفرنسي الاستيلاء على حسابات بطاقات خاصة بعملاء البنوك، لكن الشاب الفرنسي"**جان كلود** "استطاع تصميم بطاقة صرف آلي وسحب بها مبالغ من إحدى البنوك ثم ذهب إلى البنك وأعاد إليه المبالغ وأخبرهم أنه فعل ذلك ليؤكد لهم أن نظام الحماية بالبنك ضعيف ويمكن اختراقه، ولكن هذا لم يمنع الشرطة الفرنسية من القبض عليه ومحاكمته.[3] كما قامت مجموعة من الشباب الأمريكي أطلقوا على أنفسهم اسم "**الجحيم العالمي** "اختراق مواقع البيت الأبيض، والمباحث الفدرالية، والجيش ووزارة الداخلية، لكنهم لم يخربوا تلك المواقع بل اقتصر دورهم على اثبات ضعف نظم الحماية في تلك المواقع، إلا أنهم حوكموا أيضا.[4]

4. الانتقام

الانتقام يكون من قبل عمال اتجاه أنظمة المؤسسة التي يعملون بها، وهو حافز كبير يجعل العامل ينفذ هجمات ضد نظم المعلومات، كأن يحس العامل أنه ليس مقدّر على قدر كفاءته، أو أن يشعر أنه سيفقد عمله، أو المعاملة معه سيئة، كل هذه العوامل تدفعه للانتقام لذاته وتبعث البهجة في نفسه، وفي أغلب الأحيان تكون الفئة التي يدفعها الانتقام هم المستخدمون السابقون الذين طردوا من العمل، إلا أنه لا يمكن حصر هذا الدافع على هذه الفئة، فقد نجد أحيانا هذا الدافع

---

[1] Ibid, p2.

[2] Ibid, p7

[3] أسامة سمير حسين، مرجع سابق، ص 101.

[4] عبد العال الديربي، محمد صادق اسماعيل، "**الجرائم الالكترونية - دراسة قانونية قضائية-**"، المركز القومي للإصدارات القانونية، الطبعة الأولى، 2012، ص 175.

في العلاقات الخاصة بين الأفراد، وحدث الكثير من الأمثلة المشابهة كأن يختلف ثنائي بينهما فيقرصن أحدهما حساب الآخر من أجل التجسس عليه، أو تشويه سمعته أو ابتزازه.

5. المتعة أو التعلم

هناك فئة من القراصنة يدخلون لأنظمة الكمبيوتر بشكل غير قانوني لغرض الفضول واستكشاف المعلومات، وعلى الرغم من أن جرائمهم غير قانونية إلا أنها لا تهدف عموما إلى إلحاق الضرر بالبيانات أوجني المال، فهدفهم الأساسي ليس الاستفادة من جرائمهم وإنما محاولة العثور على أخطاء وثغرات الأنظمة من أجل التعلم أو اكتساب سمعة الجرأة في عملية الاختراق، أو لاحراج شخصيات في السلطة، وعليه الدافع هنا هو الفضول وحب التعلم، ومعظم الضرر المتسبب فيه يكون إما غير مقصود أوعرضي.[1]

6. الدوافع الارهابية :

الارهاب المعلوماتي هو فعل تدمير أو شراء أنظمة معلوماتية بهدف اخلال توازن بلد أو الضغط على حكومة،[2] فالتهديد الإرهابي هو كل النشاطات المنافسة التي تؤثر على توازن الأنظمة المقامة، والنشاطات التي تدخل في هذا الصنف يمكن أن تأخذ طابع عنيف كالتدمير المادي أو التلاعب بالمعلومات الحساسة، والدوافع الارهابية تكمن في تحقيق نتائج خارقة من أجل إحداث ضجّة عالمية وإحداث الحرب السيكولوجية، وتخويف الناس.[3]

ويعرف الارهاب المعلوماتي أنه استخدام التقنيات الرقمية لاخافة واخضاع الآخرين، أو مهاجمة نظم المعلومات بدوافع سياسية أو اقتصادية أو أمنية أو عرقية أو دينية.[4]

ويدخل تحت ظل الدوافع الارهابية كل المجرمين الذين يستخدمون تكنولوجيا الاعلام والاتصال للانخراط في جماعات ارهابية، الترويج للكراهية والأنشطة غير القانونية، أو الانخراط في سلوكات اجتماعية غير قانونية مثل نقل المواد الاباحية للأطفال أو الانخراط في الاعتداء الجنسي على

---

[1] Douglas Thomas & Brian D.Loader, «**Cybercrime-law enforcement, security and surveillance in the information age**-», First published, Routledge Taylor and Francis Group, 2000, pp 6-7.

[2] Didier Godart, op cit, p34.

[3] Menaces sur les systèmes informatique «Guide N 65», op cit, p10.

[4] ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي-دراسة مقارنة-، المركز العربي للنشر والتوزيع، 2017، ص92.

الأطفال عبر الانترنت، وغالبا ما تسير هذه الجماعات أو الأفراد على الخط الفاصل بين حرية التعبير والنشاط غير القانوني.[1]

الدوافع المذكورة هي أشهر الدوافع وأكثرها تسببا في ارتكاب الجرائم المعلوماتية وليست كل الدوافع الموجودة، فمع التطور التكنولوجي السريع والهائل لا يمكن حصر أنواع الجرائم المعلوماتية وبالتالي لا يمكن حصر دوافعها.

المحور الرابع: كيفية الحد من الجريمة المعلوماتية

كل المؤسسات والادارات مهما كان حجمها مستهدفة من قبل المجرمين المعلوماتيين، و للتصدي لهجماتهم وجب التحكم في ثلاث عوامل أساسية: التكنولوجيا، العامل البشري و القوانين.

1. التكنولوجيا

أول خطوة للتصدي للجريمة المعلوماتية والحد منها هي التحكم الجيد في التكنولوجيا عن طريق توفير الحماية القصوى للمعلومات المتداولة من خلالها سواء المتنقلة عبر الشبكة أو المخزنة في الحواسيب، ويكون ذلك بتركيب أحدث برمجيات الحماية، وأشهرها: برامج مكافحة الفيروسات، الجدران النارية، التشفير، التحقق من الهوية وأنظمة كشف التدخل التي يتم وضعها في أماكن أو نقاط الدخول الأكثر حساسية لشبكات المؤسسة من أجل كشف التدخلات، الاعتماد كذلك على الشبكة الافتراضية الخاصة VPN قدر المستطاع باعتبارها شبكة توفر حماية عالية لتبادل المعطيات بين موقعين متباعدين على الأقل، ضامنة بذلك هويات المرسل والمستقبل وذلك لتشفيرها حركة مرور الشبكة الحساسة عن طريق خوارزمية تشفير قوية ومعروفة، وتفرض تحقق من الهوية قوي عن طريق استعمال نظام بعاملين: اسم مستعمل وكلمة مرور.

ثانيا التحديثات التي تعتبر عملية ضرورية لفعالية البرامج، على المؤسسة الانتباه إلى أهميتها والخطورة الناتجة عن اهمالها، وتمس التحديثات كل البرامج الحساسة كنظام التشغيل، متصفح الانترنت، برامج مكافحة الفيروسات، الجدران النارية...فمثلا إذا لم يتم تحديث نظام التشغيل ضد الأخطاء والثغرات الأمنية بعد تركيب جدار ناري يمكن لأي مقرصن نشيط التنبه و استغلال الثغرة قبل تنبه المؤسسة مهما كان نوع الجدار الناري.

2.العامل البشري

للحد من الجريمة المعلوماتية لا يكفي تركيب أحدث برمجيات الحماية، فما فائدة أحدث البرامج مع مستخدم غير كفء أو غير يقظ، لذا فيقظة العامل البشري في كل تصرفاته خصوصا مستعملي

---

[1] Douglas Thomas & Brian D.Loader, op.cit, p8

التكنولوجيا مهمة جدا للتصدي لأي تدخل، ويتم تحسين فعاليته من خلال التدريب والتحسيس المستمر، والاعتماد على أحسن الكفاءات في هذا المجال.

3.تحيين التشريعات و القوانين الخاصة بالجريمة المعلوماتية

مع الأشكال الجديدة للجرائم المعلوماتية، من الضروري العمل على تطوير القوانين الوطنية في مجال مكافحة الجريمة المعلوماتية، والعمل على انشاء أجهزة متخصصة لمواجهة الاجرام المنظم، والاستفادة من التطور التكنولوجي في إجراءات جمع الأدلة للتصدي للمنظمات الاجرائية التي أصبحت تحدى أجهزة العدالة الجنائية الوطنية والاقليمية والدولية لافتقارها الآليات والأساليب التي تتناسب وطبيعة هذه الجريمة وقدرتها على التغير والتنقل بسبب مرونة هياكلها، ودقة تنظيمها والتعاون الوثيق بين أعضائها.[1]

التحكم في التكنولوجيا و العامل البشري و التشريعات لا يمكن أبدا أن يقضي على جرائم المعلوماتية وإنما يحد منها ومن آثارها الكارثية فقط، كما يجب على المؤسسات و الدول مواكبة كل التطورات التي تحدث في تكنولوجيا الاعلام والاتصال من أجل اغلاق الطريق على كل الثغرات والأبواب الجديدة للجرائم المعلوماتية.

الخاتمة

إن التطور التقني غيّر كل معالم الحياة وأثّر على كل جوانبها، حتى عالم الاجرام لم يسلم من هذا التطور، إذ أنتجت لنا المعلوماتية وكل ما يتعلق بها من أنظمة وشبكات وحواسب نوعا جديدا من الإجرام مسرحه العالم الافتراضي، حيث ظهرت أنواع جديدة من مجرمي المعلوماتية تميزهم خصائص متعددة ومختلفة عن خصائص المجرمين التقليديين، وتدفعهم دوافع عدة لارتكاب جرائمهم، منها ما تشابه مع الدوافع السابقة للاجرام ومنها ما اختلف واختص بهذه الفئة، ومن خلال هذا البحث الذي تطرقنا فيه لتعريف الجرم المعلوماتي وخصائصه وأصنافه ودوافعه تم التوصل **للنتائج** التالية:

- الجريمة المعلوماتية عبارة عن جريمة مكتملة الأركان لها خصائص تشترك فيها مع الجرائم الأخرى كالخطورة والطبيعة التي قد تكون عابرة للحدود، وخصائص أخرى تنفرد بها كوسيلة التنفيذ "الحاسوب" والتي تتطلب مهارة ومعرفة بالتقنيات، إضافة إلى صعوبة اكتشافها نظرا لحدوثها في عالم افتراضي غير ملموس.

---

[1]نقموش محمد، ميلودية أحمد، الجريمة المعلوماتية: المفهوم-حتمية تطوير آليات التعاون الدولي في مجال مكافحتها، مجلة الدراسات القانونية والسياسية، المجلد الرابع، العدد 02 جوان 2018،ص277.

- المجرم المعلوماتي وإن كان يبدو للعامة أنه أقل خطورة لابتعاده عن العنف المادي، واتسامه بصفات تجعله ذو مكانة في المجتمع، إلا أنه أكثر خطورة من المجرم التقليدي وهذا يعود لعدة أسباب:

-قدرته في الوصول إلى أشياء ومناطق يصعب على غيره الوصول إليها خصوصا في المدة الزمنية التي يستغرقها المجرم المعلوماتي، إذ يستطيع تدمير كل أنظمة المؤسسة بنقرة أو نقرتين وهو جالس في غرفته، كما يستطيع أن يمتلك ثروات طائلة دون أن يخرج من بيته أو يعرض نفسه للخطر، أو يضع نفسه موضع الشبهات.

-قدرته على التخفي وراء شاشة تصعّب من مهمة التعرف عليه وايجاده، حيث تفصل مسافات كبيرة بين الجاني والضحية، وأحيانا نجد كل منهما في بلد، إذ يحكم كل بلد قوانين مختلفة ما يخلق مشاكل في محاكمة المجرم، فما يُعتبر إجراما في بلد ما قد يعتبر أمرا عاديا في آخر، وهذا ما يجعله يخوض في هذا العالم دون خوف.

-المجرم المعلوماتي يعلم جيدا أن القوانين المتعلقة بجرائم المعلوماتية في أغلب البلدان غير متطورة ما يزيد من جرأته على ارتكاب جرائمه على عكس المجرم التقليدي الذي يحسب ألف حساب قبل الاقدام على فعلته.

-ما يجعل المجرم أكثر خطورة هو الصورة المبهمة عن شخصيته ودوافعه وهذا ما يصعب التعامل معه في حين المجرم التقليدي غالبا ما تكون دوافعه مادية.

- من الممكن الحد من هذا النوع من الجرائم عن طريق العديد من الآليات، لكن من المستحيل القضاء عليها نهائيا، فبمجرد سيطرة المؤسسة على التقنيات التي بين أيديها وسد جميع الثغرات التي يمكن أن تكون مدخلا لتهديد ما، تظهر تقنيات جديدة بثغرات جديدة وهذا هو الجانب السلبي لهذا العالم الرقمي.

التوصيات

على ضوء النتائج السابقة نقدم مجموعة التوصيات التالية:

- التكوين والتحسيس المستمر لمستخدمي التقنيات ومسؤولي الأنظمة المعلوماتية على مستوى المؤسسات، وتدريبهم على كيفية استخدام البرامج والتقنيات التي تحت أيديهم.
- استغلال المؤسسات لهذه الطاقات والمهارات الموجودة في هذه الفئات خصوصا الهاكرز لصالحها، أي تحويلهم من موضع الهجوم إلى موضع الدفاع، فالعديد من الهاكرز يسعون لتقديم خدماتهم للمؤسسات.

- ضرورة استحداث قانون جنائي مستقل للمعلوماتية في التشريعات الوطنية.
- تحيين القوانين بما يتناسب مع التطور السريع الذي يشهده العالم الرقمي.

التنظيم القانوني لتكنولوجيـات الإعلام والاتصـال و الحماية المقررة لها

أ. د. حساني علي

أستاذ محاضر بجامعة ابن خلدون - تيارت

مقدمـــــــــــــــــة:

لاشك أن العالم العربي بصفة عامة والجزائر خاصة انتبهت الى ما يجري في العالم وما يدور حولها من تطور ملفت للنظر في كل المجالات، وما صاحب هذا التطور من تحدي وصراعات لتولي السيادة في التحكم العالمي لمجريات الاحداث والتوازنات العالمية الخطيرة التي هدفها الاسمى والرئيس هو المصلحة ولا شيء غير المصلحة.

إن التسارع الذي نشهده الان في العالم كان سببه ولايزال هو رفع مستوى تقنية المعلومات والتكنولوجيا المرتبطة بها، ولاشك أن الاتصالات أدت إلى تغير لغة المنافسة العالمية وشكلت تحديات ضخمة على منظمات الأعمال والادارة... وللانسجام مع هذه التغييرات اهتمت الدول العربية بالنظر باهتمام لمواردها المعرفية وابتكار وسائل اتصال جديدة لأنشطة أعمالها بعدما أحدثت الثورة التكنولوجية تأثيرات هائلة على أنماط الإنتاج والاستثمار والاستهلاك والادارة العامة وغيرها من القطاعات، فأخذت نتعامل مع الكمية الهائلة من المعلومات والمعرفة في محاولة منها لخزنها واستعمالها من خلال مشاركتها مع الآخرين داخل دولة معينة وخارجها والاستعانة بتكنولوجيا المعلومات لجعلها سهلة الاستعمال والتداول في خطوة للمساهمة في بناء اقتصاد المعرفة.

أولاً: مشكلة الدراسة والأسئلة المرتبطة بها

يمكن صياغة مشكلة الدراسة من خلال طرح الاسئلة الآتية :

1- ماهي المفاهيم المرتبطة بتقنية المعلومات وتكنولوجيات الاعلام والاتصال، سواء ما جاءت به الاتفاقية العربية من مصطلحات او القانون 04/09 او الفقه بصفة عامة.

2- هل هناك فجوة معرفية بين الدول العربية ومن بينها الجزائر وبين الدول الصناعية المتقدمة تمثل بالنقص في التعامل مع تقنية وتكنولوجية المعلومات من خلال مكافحة الجرائم المتصلة بها ؟ .

3- هل ساهم قانون العقوبات الجزائري في الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ؟.

4- هل تساهم تقنية المعلومات وتكنولوجيا الاعلام والاتصال في تكوين المحتوى المعرفي المناسب للدول العربية بما يمكنها من المساهمة العلمية والتكنولوجية ؟.

5- هل يكفي استغلال تكنولوجيا المعلومات والاتصال دون وضع الاطر اللازمة لمحاربة الجرائم المرتبطة بها ووضع السبل الناجعة للوقاية من هذه الجرائم؟.

ثانياً: أهداف الدراسة

انطلاقاً من اسئلة الدراسة فإن اهداف هذه الدراسة تتلخص بالآتي :

1- تحديد النصوص القانونية في الجزائر والاتفاقية العربية لمكافحة جرائم تقنية المعلومات ودراستها بعمق.

2- تحديد المعوقات والصعوبات التي تواجهها البلدان العربية في مجال تقنية المعلومات في ظل التطورات التكنولوجية العالمية المتسارعة .

3- محاولة تحديد التصورات التي يمكن ان تكون عليها متطلبات الأطر والوسائل المهمة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

4- معرفة القواعد الاجرائية المتخذة من قبل السلطات والمصالح المختصة والمتعلقة منها بالتفتيش والحجز وكذا الحصول على المعطيات المخزنة في منظومة معلوماتية.

5- معرفة الحالات التي تسمح باللجوء الى المراقبة الالكترونية.

6- الاحاطة بالتزامات ومهام مقدمي الخدمات.

7- دور ومهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته.

ثالثاً: مفاهيم ومصطلحات الدراسة

من خلال دراستنا لموضوع تقنية المعلومات وتكنولوجيات الاعلام والاتصال، اتضح لنا ضرورة تثبيت بعض المفاهيم التي تخدم البحث وهدفه والمستخدمة في هذا الشأن، ومنها ما يلي :

1- **تقنية المعلومات:Systemeinformatique** أية وسيلة مادية او معنوية اومجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا او لاسلكيا في نظام او شبكة.

2- **مزود الخدمة:Fournisseurdeservice**أي شخص طبيعي او معنوي عام او خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات او مستخدميها.

3-**البيانات:Données**كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما اليها...

4- **البرنامج المعلوماتي:Programmeinformatique**مجموعة من التعليمات والاوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لانجاز مهمة ما.

5- **النظام المعلوماتي:Logicielinformatique**مجموعة برامج وادوات معدة لمعالجة وادارة البيانات والمعلومات.

6- **الشبكة المعلوماتية:Reseauinformatique**ارتباط بين اكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

7-**الموقع:Cite**إمكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

8-**الالتقاط:** مشاهدة البيانات او المعلومات او الحصول عليها.

9-**معلومات المشترك:** أية معلومات موجودة لدى مزود الخدمة المتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:

أ) نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.

ب) هوية المشترك وعنوانه البريدي او الجغرافي او هاتفه ومعلومات الدفع المتوفرة بناء على اتفاق او ترتيب الخدمة.

ت) أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة[1].

10- **الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: Infractions liées aux technologies de information et de la communication(TIC)**جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات وأي جريمة اخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية.

11- **منظومة معلوماتية:Systemeinformatique**أي نظام منفصل او مجموعة من الانظمة المتصلة ببعضها البعض او المرتبطة، يقوم واحد منها او اكثر بمعالجة الية للمعطيات تنفيذا لبرنامج معين.

---

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 2010/12/21.

12- **معطيات معلوماتية:Données informatique**أي عملية عرض للوقائع او المعلومات او المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

13- **مقدمو الخدمات**:- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات. - وأي كيان اخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمات الاتصال المذكورة أو لمستعمليها.

14- **المعطيات المتعلقة بحركة السير**: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الاخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

15- **الاتصالات الالكترونية:Communication electronique** أي تراسل او ارسال أو استقبال علامات او اشارات او كتابات اوصور او اصوات او معلومات مختلفة بواسطة اي وسيلة الكترونية[1].

رابعاً: إشكالية البحث

من خلال ما تم عرضه ولغرض القاء الضوء على هذا الموضوع نطرح الاشكال التالي:

ماهي الاطر القانونية التي تحكم تقنية المعلومات، وماهي الوسائل المتخذة للوقاية من الجرائم المرتبطة بها ومكافحتها تبعاً لأحكام الاتفاقية العربية وقانون 04/09.

خامساً:: خطة البحث

ومن أجل البحث في الاشكالية ومحاولة الاجابة عنها عن طريق هذه الورقة البحثة قسمنا دراستنا الى مبحثين اساسين هما:

1-التنظيم القانوني لتكنولوجيات الاعلام والاتصال وتقنية المعلومات والمفاهيم المرتبطة بها في مبحث أول.

2- الجرائم الماسة بتكنولوجيات الإعلام والاتصال وتقنية المعلومات ومكافحتها في مبحث ثاني.

المبحث الأول : التنظيم القانوني لتكنولوجيات الإعلام والاتصال وتقنية المعلومات والمفاهيم المرتبطة بها

المطلب الاول: المعلومة

---

[1] م2 من قانون 04/09 المؤرخ في 2009/08/05 يتظمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها(ج ر 47 بتاريخ 2009/08/16).

اولا: تعريف المعلومة وأهميتها

تشكل المعلومة العصب المحرك لأي نشاط يقوم به إنسان في ممارساته اليومية على اختلاف مجالات استخدامها ، و نظرا للتداخل بين مفهوم كل من المعلومات و البيانات ،سوف يتم التعرف على كل واحد منها على حدا.

أ-البيانات

تعرف البيانات بكونها :" المادة الخام اللازمة لإنتاج المعلومات وذلك طبقا لمفهوم النظام بحيث تمثل البيانات المدخلات و المعلومات المخرجات و هذا بعد المعالجة"[1] .

كما أنها:"هي عبارة عن تعبيرات لغوية او رياضية او رمزية او مجموعة منها و يتم التعارف على استخدامها لتمثل الأفراد و الأشياء و الأحداث و المفاهيم أي تشير البيانات لأي حقائق خام او مشاهدات و التي تصف ظاهرة معينة ويرى ان المعلومات هي عبارة عن بيانات وضعت في محتوى ذات معني و دلالة لمتلقيها بحيث يخصص لها قيمة لأنه يتأثر بها او لأنها تحقق له منفعة"[2].

من خلال هذين التعريفين يتضح أن البيانات تشكل المادة الخام الأساسية الذي تنتج منها المعلومة.

ب- المعلومة

أما المعلومة فهي: " عبارة عن بيانات تم تصنيفها و تنظيمها بشكل يسمح باستخدامها والاستفادة منها"[3]. إذن هي البيانات التي يمكن الحصول عليها عند حدوث ظاهرة او موقف، ويتم معالجتها وتحويلها الي معلومة تخدم الموقف.

وهي أيضا: " أساس المعرفة ومزودها بالمعطيات والبيانات والرموز، ومخزونها من الوثائق والأرشيفات وبنوك المعطيات التي ترويها وتغذيها والمعرفة امتداد للمعلومة تصفى ما توفر منها هيكله تحدد له السيروره وتضع له السياق"[4].

---

[1] إبراهيم بختي، تكنولوجيا و نظم المعلومات في المؤسسات الصغيرة و المتوسطة،على الخط: http://bbekhti.online.fr/trv_pdf/TIC.pdf,29/04/2008,09:58.

[2] ثابت عبد الرحمن ادريس، نظم المعلومات الادارية في المنظمات المعاصرة ،الدار الجامعية، الاسكندرية،2005،ص68-69.

[3] إبراهيم بختي، المرجع اعلاه.

[4] يحي اليحياوي، على الخط : http://www.trcsr.com/detail.php?id=7 2008/04/24 13:23

وفقا لهذا التعريف يتضح أن المعلومة حاملة للمعرفة والمعرفة حاضنة للمعلومة يلتقيان في الهدف ويتقطعان في الغاية.

2- اهمية المعلومة

اقدر الناس على التخطيط والتعامل مع الأشياء هم من يمتلكوا المعلومات بمختلف صورها و أشكالها، فالمعلومة ذات أهمية بالغة و التي تظهرها النقاط التالية[1]:

- إدراك الظروف المحيطة بناء سواء في الحياة الخاصة او العامة، وفي الإدارة على اختلاف مجالاتها ومستوياتها، او في مجال البحث العلمي، او في مجال الدفاع الوطني والأمن القومي .
- إدراك ما يطرأ على الظروف المحيطة من تغير، والتعرف على ابعاد هذا التغير وطبيعته.
- التعرف على سبل التعامل مع هذا التغير، او تطويقه، او التأقلم معه، الى غير ذلك من البدائل المختلفة حسبما تملي ظروف الموقف.
- تحديد البديل المناسب، واتخاذ القرار بشأنه.
- تنفيذ القرارات.
- متابعة نتائج التنفيذ.

ثانيا: خصائص المعلومة ومصادرها

1-خصائصها

عادة ما تكون المعلومة مرتبطة بحدث أو موقف لذا نجد أنها تختلف باختلاف الموقف فقد تكون كمية، وصفية، رقمية...الخ ، و قد حدد **Bruch**وزملائه عشرة خصائص أساسية للمعلومات وذلك على النحو التالي[2]:

- **التوقيت**: ومعني هذا عدم وصول المعلومات لمتخذ القرارات بعد الحاجة لها او قبل ذلك بفترة طويلة لاحتمالات تقادمها.
- **الدقة**: وتكون في إجراءات القياس المستخدمة في إعداد المعلومات و تشغيلها وتجهيزها وتلخيصها و عرضها.
- **الصحة**: أي درجة خلو المعلومات من الأخطاء سواء كانت لغوية او رقمية.
- **إمكانية التعبير الكمي**: إمكانية التعبير عن المعلومات بالأرقام و النماذج الكمية إذا لزم الأمر.

---

[1] إبراهيم بختي، تكنولوجيا و نظم المعلومات في المؤسسات الصغيرة و المتوسطة،على الخط: http://bbekhti.online.fr/trv_pdf/TIC.pdf,29/04/2008,09:58

[2]- ثابت عبد الرحمن ادريس، المرجع السابق،ص80-81

- **إمكانية التحقق**: درجة الاتفاق فيما بين المستخدمين المختلفين عندما يتفحصون نفس المعلومات.
- **إمكانية الحصول عليها**: والمقصود درجة اليسر والسرعة في الحصول على المعلومات الأزمة .
- **الخلو من التحيز**: أي غياب النية في تعديل او تحريف المعلومات للتأثير على المتلقيا و لتحقيق أغراض خاصة.
- **الشمول**: اكتمال المعلومات.
- **الملائمة**: مدى ارتباط المعلومات بمتطلبات المستخدم المحتمل لها.
- **الوضوح**: مدى خلو المعلومات من الغموض.

2-مصادرها :للمعلومة عدة مصادر وهي[1]:

-الملاحظة: يمكن الحصول على أجوبة جزئية لمشكل معين عن طريق ملاحظة الأحداث المرتبطة به.

-التجربة: وذلك عن طريق إخضاع مصادر المعلومات (الأفراد ،الآلات ، الأنشطة...الخ) لتجارب تخضع للحكم، وكلما كان تصميم التجربة جيدا كلما كانت النتائج موثوق فيها أكثر.

-المسح: وهو مصدر معلومات فني يحتاج الى التخطيط الجيد والخاصة فيما يخص إعداد قوائم الاستبيان و اختيار العينة، و يكتسي هذا المصدر أهمية بالغة في الدراسات التسويقية .

-المؤسسة: من خلال مختلف التقارير التي يعدها أجزائها و هو مصدر هام جدا خاصة من خلال إنتاجه للمعلومات التي تصحح الانحرافات التي قد تعرض له المؤسسة.

-البيئة الخارجية للمؤسسة: يتمثل في المعلومات التي يمكن الحصول عليها من مكاتب البحوث الإحصاء الاستشارات والنشرات المختلفة لهيئات خاصة او حكومية لكن يجب توخى الحذر في استعمال مثل هذه المعلومات ولا يجب اعتبارها في جميع الأحوال صحيحة بصفة مطلقة كما أن تعدد مصادر المعلومة الواحدة مفيدة جدا في تقييم مدى دقتها و تمثيلها للواقع.

ثالثا: منافع المعلومة : تساهم المعلومة في تحقيق منافع تؤدي الى تسهيل او تعقيد استخدام المعلومة ذاتها ويمكن ان نفرق بين ثلاثة منافع أساسية و هي[2]:

---

[1]- إبراهيم بختي، تكنولوجيا ونظم المعلومات في المؤسسات الصغيرة والمتوسطة، على الخط: http://bbekhti.online.fr/trv_pdf/TIC.pdf,29/04/2008,09:58.

[2]بول جامبل، جون بلاكويل، ادارة المعلومات، دار الفاروق، مصر، 2003، ص16.

-**المنفعة الشكلية** : و تعبر عن مدى صياغة المعلومات في الشكل او الصورة التي تتفق واحتياجات وقدرات المستخدم المتوقع لها، فقد يعبر عنها في صورة جداول او رسوم بيانية او صور معادلات رياضية...الخ

-**المنفعة الزمنية** : يتم توفير المعلومات في الوقت الحاجة إليها لاتخاذ القرارات الملائمة .

-**المنفعة المكانية** : حيث يصبح للمعلومات قيمة اعلى عندما يتم الحصول عليها في المكان المناسب

-**المنفعة الحيازية** : يصبح للمعلومات قيمة اعلى عندما يتم حيازتها بواسطة متخذي القرارات .

المطلب الثاني: تعريف نظام المعلومات

تعمل المؤسسة على جمع المعلومات، وتحولها، لتنتج أخرى جديدة، وتعد المعلومة مورد مكلف للمؤسسة ومؤثرا في نفس الوقت بحياتها، لأن أي حركة داخلية أو خارجية لها أثر رجعي يولد معلومات في صورة كمية أو نوعية. وحتى تتم عملية إنتاج المعلومة واستعمالها يجب أن يتوفر ما يسمى بنظام المعلومات.

ويمثل نظام المعلومات:" النظام الذي يجمع ويحول ويرسل المعلومات في المنشاة ويمكن أن يستخدم أنواعا عديدة من نظم المعلومات لمساعدته على توفير المعلومات حسب احتياجات المستفيدين"[1].

إذن فهو يعمل على توفير المعلومات التي يحتاج لها المديرون لاتخاذ القرارات الخاصة بفعالية وبالتالي رفع مستوى الأداء وتحقيق الأهداف التنظيمية.

وكما يعرف أيضا بأنه :" مجموعة متجانسة ومترابطة من الأعمال، العناصر والموارد تقوم بتجميع تشغيل إدارة ورقابة البيانات بغرض الإنتاج وتوصيل معلومات مفيدة لمستخدمي القرارات من خلال شبكة من خطوط القنوات الاتصال" [2].

فنظام المعلومات هو عبارة عن عملية إنتاج وتجهيز وتدبير المعلومات والأنشطة والقنوات في بيئة معينة بهدف تداولها في هـذه البيئة.

المطلب الثالث: ماهية تكنولوجية المعلومات

أولا: تعريف تكنولوجية المعلومات

---

[1]علي محمد منصور، مبادئ الإدارة"، أسس ومفاهيم"، الطبعة الأولى، مجموعة النيل العربية، القاهرة، 1999،ص85.

[2]إبراهيم بختي ، تكنولوجيا و نظم المعلومات في المؤسسات الصغيرة و المتوسطة، على الخط : المرجع السابق.

لم تحض تكنولوجية المعلومات - كغيرها من المصطلحات الجديدة - خاصة مع ظهور الاقتصاد الجديد بتعريف موحد، بل تعددت هذه التعاريف وتنوعت تبعا لرؤية كل واحد لها، لذا سندرج عدة تعاريف حتى تبرز لنا أوجه الاختلاف والاتفاق فيما بينها.

التعريف الأول: « تكنولوجية المعلومات هي استعمال التكنولوجية الحديثة للقيام بالتقاط ومعالجة، وتخزين واسترجاع، وإيصال المعلومات سواء في شكل معطيات رقمية، نص، صوت أو صورة».[1]

التعريف الثاني:« جميع أنواع التكنولوجية المستخدمة في تشغيل، ونقل وتخزين المعلومات في شكل إلكتروني وتشمل تكنولوجية الحاسبات الآلية ووسائل الاتصال وشبكات الربط وأجهزة الفاكس وغيرها من المعدات التي تستخدم بشدة في الاتصالات».[2]

من خلال التعاريف السابقة نستنتج عنصرين هامين:

الأول: أن تكنولوجية المعلومات هي حقل من حقول التكنولوجية والتي تهتم بمعالجة المعلومات.

الثاني: التركيز على عمليات الاستقطاب، التخزين والمعالجة (المعلوماتية)، وعملية البث (الاتصال).

ثانيا : خصائص تكنولوجيا المعلومات

لقد تميزت تكنولوجية المعلومات عن غيرها من التكنولوجيات الأخر بمجموعة من الخواص أهمها:[3]

1 - **تقليص الوقت**: فالتكنولوجية جعلت كل الأماكن - إلكترونيا - متجاوزة؛
2 - **تقليص المكان**: تتيح وسائل التخزين التي تستوعب حجما هائلا من المعلومات المخزنة والتي يمكن الوصول إليها سهولة؛
3 - **اقتسام المهام الفكرية مع الآلة**: نتيجة للتفاعل بين الباحث والنظام.
4 - **النمنمة**: بمعنى آخر، أسرع، أرخص ...إلخ، وتلك هي وتيرة تطور منتجات تكنولوجية المعلومات؛

---

[1]:مراد رايس،أثر تكنولوجية المعلومات على الموارد البشرية في المؤسسة،رسالة ماجستير في علوم التسييرفرع إدارة الأعمال ،جامعة الجزائر2005- 2006 ص: 28

[2]سعاد بومايله وفارس بوباكور، أثر التكنولوجيات الحديثة للإعلام والاتصال في المؤسسة الاقتصادية، مجلة الاقتصاد المناجمت، العدد 03، مارس 2004، ص 205.

[3]مراد رايس ، مرجع سابق ، ص : 29

5 - **الذكاء الاصطناعي**: أهم ما يميز تكنولوجية المعلومات هو تطوير المعرفة وتقوية فرص تكوين المستخدمين من أجل الشمولية والتحكم في عملية الإنتاج؛

6 - **تكوين شبكات الاتصال**: تتوحد مجموعة التجهيزات المستندة على تكنولوجية المعلومات من أجل تشكيل شبكات الاتصال، وهذا ما يزيد من تدفق المعلومات بين المستعملين والصناعيين، وكذا منتجي الآلات، ويسمح بتبادل المعلومات مع باقي النشاطات الأخرى.

7 - **التفاعلية**: أي أن المستعمل لهذه التكنولوجية يمكن أن يكون مستقبل ومرسل في نفس الوقت، فالمشاركين في عملية الاتصال يستطيعون تبادل الأدوار وهو ما يسمح بخلق نوع من التفاعل بين الأنشطة؛

8 - **اللاتزامنية**: وتعني إمكانية استقبال الرسالة في أي وقت يناسب المستخدم، فالمشاركين غير مطالبين باستخدام النظام في نفس الوقت؛

9 - **اللامركزية**: وهي خاصية تسمح باستقلالية تكنولوجية المعلومات والاتصالات، فالانترنيت مثلا تمتع باستمرارية عملها في كل الأحوال، فلا يمكن لأي جهة أن تعطلها على مستوى العالم .

10 - **قابلية التوصيل**: وتعني إمكانية الربط بين الأجهزة الاتصالية المتنوعة الصنع، أي بغض النظر عن الشركة أو البلد الذي تم فيه الصنع؛

11 - **قابلية التحرك والحركية**: أي أنه يمكن للمستخدم أن يستفيد من خدماتها أثناء تنقلاته، أي من أي مكان عن طريق وسائل اتصال كثيرة مثل الحاسب الآلي النقال ، الهاتف النقال ...إلخ.

12 - **قابلية التحويل**: وهي إمكانية نقل المعلومات من وسيط إلى آخر، كتحويل الرسالة المسموعة إلى رسالة مطبوعة أو مقروءة مع إمكانية التحكم في نظام الاتصال.

13 - **اللاجماهرية**: وتعني إمكانية توجيه الرسالة الاتصالية إلى فرد واحد أو جماعة معنية بدل توجيهها بالضرورة إلى جماهير ضخمة، وهذا يعني إمكانية التحكم فيها حيث تصل مباشرة من المنتج إلى المستهلك، كما أنها تسمح بالجمع بين الأنواع المختلفة للاتصالات. سواء من شخص واحد إلى شخص واحد، أو من جهة واحدة إلى مجموعات، أو من مجموعة إلى مجموعة.

14 - **الشيوع والانتشار**: وهو قابلية هذه الشبكة للتوسع لتشمل أكثر فأكثر مساحات غير محدودة من العالم بحيث تكتسب قوتها من هذا الانتشار المنهجي لنمطها المرن.

15 - **العالمية:** وهو المحيط الذي تنشط فيه هذه التكنولوجيات، حيث تأخذ المعلومات مسارات مختلفة ومعقدة تنتشر عبر مختلف مناطق العالم، وهي تسمح لرأس المال بأن يتدفق إلكترونيًا خاصة بالنظر إلى سهولة المعاملات التجارية التي يحركها رأس المال المعلوماتي فيسمح لها بتخطي عائق المكان والانتقال عبر الحدود الدولية.

ثالثا : المجالات الاقتصادية لتطبيق تكنولوجيا المعلومات : ساعدت التكنولوجيا بصفة عامة المجتمعات في ممارسة أعمالهم اليومية بسهولة، و تكنولوجيا المعلومات في الآونة الأخيرة لم تترك مجتمعا إلا و اقتحمت جميع أنشطته سواء السياسية او المدنية ، العسكرية ، التجارية ، التعليمية ،....و باتت بذلك تطبيقاتها غير محدودة و لا متناهية و بل و شملت الميادين التي عجز الإنسان عن اقتحامها ففتحت بذلك آفاقا جديدة و أوجدت مجالات حديثة للبحث .

ويمكن الإشارة إلى بعض التطبيقات التي مست علم الاقتصاد على سبيل المثال لا الحصر في ما يلي[1]:

1 - **قطاع المال والاقتصاد:**

- إكمال أعمال البنوك : من اجل تحسين الخدمة بشكل عام ،و سرعة الضبط للحسابات، بالإضافة الى مساندة الرقابة المالية على البنوك.
- تحويل الأموال إلكترونيًا: والهدف منه سرعة الخدمة، تقليل العمل الورقي للعمليات بين البنوك.
- إقامة النماذج الاقتصادية لتحليل أداء النظم الاقتصادية وتقييم الإستراتيجيات.
- إدارة الاستثمارات: بتعظيم عائد الاستثمارات، وتحليل المخاطر.
- تنظيم معلومات أسواق الأوراق المالية من خلال فورية بث المعلومات للمتعاملين و استخراج إحصائيات السلاسل الزمنية لتغير أسعار الأسهم والسندات والمؤشرات الاقتصادية الأخرى.
- التصميم بمساعدة الكمبيوتر: لسرعة تعديل وتعدد تجارب التصميم وتوفير جهد ما بعد التصميم من خلال قيام النظام الآلي بتحديد قوائم المكونات والمواد الداخلة فيه.

2 - **مجال التعليم والتدريب :**

- نظم التدريب من خلال المحاكاة لرواد الفضاء والطيارين على قيادة المركبات وهذا ما يقلل التكاليف والخطر.

[1] كمال عبد الحميد زيتون ، تكنولوجيا التعليم في عصر المعلومات و الاتصال ، عالم الكتب ، القاهرة،مصر،2002، ص ص: 159-161

- برمجيات مساندة التعليم و التعلم: الهدف منها زيادة إنتاجية المعلم والطالب في مواجهة تضخم المادة التعليمية وتعقدها.
- نظم المعلومات التربوية، والتي تساعد على صياغة ووضع السياسات التربوية والتخطيط التربوي وجهود البحوث و التنظير في مجال التعليم.

هذا وغيرها من المجالات التي مستها هذه التكنولوجيا، ولا تعتبر نوعا من المبالغة إذا قلنا أنها مست مختلف مجالات الحياة بدون إستثناء(الطب والدواء، النقل والمواصلات، الأمن والقانون، الإعلام، البيئة ...إلخ).

المطلب الخامس: تكنولوجيا الاتصال وشبكات المعلوماتية

أولا : تكنولوجيا الاتصال

1- الاتصال

قد شهد العالم في السنوات الأخيرة تطورا مذهلا في وسائل وتكنولوجيا الاتصالات، وأصبح من الصعب متابعة المخترعات الجديدة في هذا المجال فلقد تطور الهاتف إلى التيلكس، والفيديو الذي تطور إلى الفيديوتكس ودخلنا عصر الأقمار الصناعية وعصر الانترنت والبريد الإلكتروني، ولا يزال التطور مستمرا في هذا المجال مما جعل العالم قرية صغيرة عن طريق استخدام وسائل للاتصال (تكنولوجيا الاتصال) متنوعة الأشكال نذكر منها على سبيل المثال لا الحصر :[1]

2- التلكس والتليتكس .

- **التلكس Télex**

وهو:" نظام لنقل الرسائل باستخدام جهاز يسمى المبرقة وهي أول جهاز تم استخدامه في إرسال الرسائل بالكهرباء. ومعظم رسائلها كان يتم إرسالها في وقت من الأوقات بتخصيص شفرة معينة لكل حرف عن طريق مفتاح المبرقة ثم تقوم هذه الأخيرة بتحويل النقط (...) والشرطات (--) الخاصة بالشفرة إلى نبضات كهربائية وإرسالها عبر أسلاك البرق. وتعرف الشفرة الخاصة بالمبرقة (شفرة مورس)"[2].

---

[1] لمين علوطي ،مرجع سابق ، ص ص : 23-30 .

[2] ربحي مصطفى عليان ومحمد عبد الدبس، وسائل الاتصال وتكنولوجيا التعليم، دار الصفاء، الأردن، 1999، ص 106.

في أواخر القرن ظهرت الوسائل والمعدات التي يتم استخدامها في شكل مطبوع بدلا من إشارة (مورس). وفي بداية القرن العشرين بدأ استخدام وسائل إرسال واستقبال الرسائل بواسطة الشرائط المثقبة. وفي العشرينيات من القرن العشرين تم استخدام الطابعات عن بعد (التلبرنتر) التي بإمكانها إرسال نبضات كهربائية مباشرة عبر خطوط البرق إلى مبرقة أخرى على الطرف الآخر من الخط.

لقد ساهم التلكس في نقل الرسائل والأنباء الصحفية وكان لسنوات طويلة هو العصب الرئيسي للتجارة وأعمال الحكومة والأعمال الحربية. وعندما صارت خدمة الهاتف في متناول الأفراد والمؤسسات تم الاستغناء عن خدمات التلكس لحد كبير، واستبدال التلكس بمعدات اتصال أخرى أسرع ولها القدرة على التعامل مع أنواع مختلفة من الرسائل والمعلومات.

- **التليتكس (تبادل النصوص عن بعد Télétex:**

يعد نظام تبادل النصوص عن بعد أو ما يسمى بالتلتكس حالة متقدمة على نظام المبرقة وتطويرا لها، حيث أنه يجمع بين عمل التلكس الاعتيادي وعمل نظام معالجة النصوص، الذي يعمل بواسطة الآلة الكاتبة الإلكترونية والشاشة المرئية المثبتة فيها، مع وجود إمكانية لخزن المعلومات المطبوعة. وبذلك يمكن إعداد نص كامل من المعلومات بواسطة الآلة الكاتبة، ثم قراءته على الشاشة وتعديله قبل إرساله إلى المستقبل أو الجهات المعنية في أي وقت لاحق. وهذا يعني أن تبادل الرسائل والمعلومات يكون إلكترونيا من وحدة ذاكرة (Mémoire) إلى وحدة ذاكرة ثانية أو أكثر وعبر شبكة اتصالات.

ويعمل التليتكس بجهازين (واحد للإرسال، وآخر للاستقبال) محدودة القدرة، أي أنها ترسل 6-7 حروف في الثانية، مع إمكانية الطباعة على الورق العادي، ورقة ورقة، حيث يمكن نقل 2400 وحدة في الثانية أي 50 مرة نظريا أسرع من التيلكس، ويتميز التيلتكس على التلكس فيما يلي:

1. سرعة تناقل المعلومات والتراسل. (تعادل ما يقارب 50 مرة سرعة التلكس العادي)
2. كمية أكبر من الرموز المستخدمة - بمعدل (307) رمز مقارنة مع 47 رمزا في نظام التلكس
3. يكون إرسال المعلومات بشكل صفحة متكاملة، وهذا أفضل من نظام الكلمات والجمل المغنطة في نظام التلكس
4. يمكن إرسال الرسالة أو النص المطلوب إلى عدة مستفيدين وفي وقت واحد

5. يوفر تبادلا محليا وإقليميا ودوليا للمعلومات أسرع وأفضل من نظام التلكس.

وبشكل عام يمكن استخدام التليتكس في المجالات التالية:

- المراسلات: مثل المذكرات والتقارير والرسائل العامة أو المخصصة في مجال معين؛
- الشؤون الإدارية: مثل وثائق الموظفين، جرد المخازن، اعتماد النماذج و الطلبيات؛
- الشؤون المالية: كالحسابات الجارية، وقوائم الأسعار، وتسجيل المبيعات والصفقات؛
- مجالات أخرى: مثل الإعلانات التجارية، القوائم التفصيلية للمؤسسات والمعلومات المرجعية.

3- الهاتف وبنوك الاتصال المتلفزة

أ- الهاتف وخطوطهTéléphone

يمثل الهاتف من أهم وسائل الاتصال الصوتي ومن أقدمها وأكثرها انتشارا بين الناس، والهاتف ليس أداة للتواصل بين الأفراد والجماعات، ولكنها أداة تلعب دورها في الإنتاجية والتسويق وإيصال الخدمات للكثير من المؤسسات، وينظر إليه كقناة اتصال غير مباشر بين الراسل والمستقبل عند مزاولة عملية الاتصال وقد تطور الهاتف في حجمه وشكله ومزاياه وإمكاناته عدة مرات.

وأصبحت هناك شبكات هاتفية من أحدث الابتكارات في عالم الاتصالات الهاتفية الهاتف الصوري أو الهاتف الفيديو الذي يستطيع نقل الصورة مع الصوت بسرعة هائلة، وهو مزود بذاكرة تؤهله لخزن الصور واسترجاعها عند الحاجة ومشاهدتها على الشاشة أو طباعتها على الورق وينتشر حاليا الهاتف النقال بشكل واسع بين الناس. ويستخدم الهاتف كوسيلة اتصال بالهواتف الأخرى المنتشرة جغرافيا بطريقتين أساسيتين:[1]

1- طريقة الاتصال المباشر: من المتحدث على الهاتف (أ) إلى متحدث آخر على الهاتف (ب)؛

2- طريقة الاتصال غير المباشر: وذلك عن طريق ربط الخط الهاتفي مع وسيلة أخرى من وسائل الاتصال ونقل المعلومات مثل التلكس والحواسيب وغيرها.

ويمكن للاتصال الهاتفي (المباشر وغير المباشر) أن يكون بشكلين أساسيين هما:[2]

1) الاتصال السلكي: عبر الأسلاك الموصلة بين الهواتف المختلفة، وعبر محطات مركزية تنتشر في المدينة أو المؤسسة؛

---

[1] عامر ابراهيم قنديلجي ، ايمان فاضل السمرائي ، تكنولوجيا المعلومات و تطبيقاتها ، الوراق ، عمان الاردن ،2002،ط1، ص،216.

[2] لمين علوطي ،مرجع سابق ، ص : 25 .

2) الاتصال اللاسلكي: دون الحاجة إلى وجود أسلاك، وعن طريق البث والتوصيل للأمواج الأرضية أو الاتصالات الفضائية.

وهناك طريقتان تستخدمان لنقل الكم الهائل من المعلومات بين الهواتف:[1]

1) طريقة استخدام الكابل : الذي يضم عددا من الأسلاك النحاسية عالية التحميل، أي القادرة على نقل كميات هائلة من الرسائل والمعلومات. تستخدم كذلك في نقل المعلومات والصور والبرامج التلفزيونية بين الحواسيب وهناك الكابل البحري الذي يربط بين الدول والقارات.

2) أما الميكروويف أو الموجات الدقيقة، فهي وسيلة أخرى مهمة لنقل المعلومات الصوتية أو المكتوبة أو لمرئية بين المناطق الجغرافية المتباعدة. وهو نوع من الاتصالات اللاسلكية الأرضية التي تتم عن طريق هوائيات وأبراج توضع في مناطق مرتفعة وعلى مسافة تقرب من 50 كلم بين كل هوائي وآخر. و يمكنه نقل 10 آلاف خط هاتفي، ويمتاز بقلة تكلفته. إلا انه يتعرض في الأحوال الجوية الماطرة للتشويش.

ومع التطورات التي تشهدها وسائل وتكنولوجيا الاتصال، أخذت الاتصالات الهاتفية تحول إلى نظام جديد رقمي يعمل عن طريق ترجمة موجات البث الإلكتروني إلى جزيئات تفصل بينهما مسافات. وهذه الجزيئات هي نتاج الأرقام الثنائية، وهي أصغر الوحدات في معالجة البيانات؛ ويعتبر هذا النوع من الأنظمة أكثر دقة وفعالية ويمكن الاعتماد عليه أكثر من وسائل الاتصال التقليدية، وهو مناسب لمختلف أنواع الاتصالات و الأكثر ملائمة للاتصال مع الحواسيب. بالإضافة إلى أنه يعطي نوعية أفضل بالنسبة للصوت والصورة المنقولة.

ب- بنوك الاتصال المتلفزة:[2]

تعد بنوك الاتصال المتلفزة أو ما يطلق عليها مصطلح الفيديوتكس (أو الفيديوتكست) من تقنيات الاتصال الحديثة المستخدمة في نقل الرسائل والمعلومات بين الأفراد والمؤسسات، وهي حالة متطورة لاستخدام واستثمار جهاز التلفزيون العادي عن طريق إضافة محطات وقنوات جديدة إلى جانب قنواته الاعتيادية. ويعرف الفيديوتكس على أنه وسيلة لعرض الكلمات والأرقام والصور والرموز على شاشة التلفزيون عن طريق ضغط مفتاح معين ملحق بجهاز التلفزيون.

---

[1] عامر إبراهيم قنديلجي، إيمان فاضل السامرائي ،مرجع سابق ،ص ص: 212-215 .

[2] . ربحي مصطفى عليان عبد الدبس، مرجع سابق ، ص 111 .

ويشمل تقنية الفيديوتكس على ثلاث ركائز مهمة هي:[1]

1. البث عن طريق شاشة تلفزيونية؛
2. تخزين واسترجاع عن طريق الحاسوب؛
3. نقل هاتفي أو بوسيلة سلكية أو لا سلكية.

وتشمل بنوك الاتصال المتلفزة (الفيديوتكس) على نوعين رئيسيين هما:

1. الفيديوتكس العادي أو الإذاعي ويسمى التليتكست (Télétex) أو النص المتلفز.
2. الفيديوتكس المتفاعل ويسمى أيضا بخدمة البيانات المرئية.

3- الفاكسميلي (الناسخ الهاتفي) Facs mile والأقمار الصناعية :

- **الفاكس (الناسخ الهاتفي) :**

وهو:"جهاز يقوم ببث الرسائل والنصوص والصور والوثائق المكتوبة عبر خطوط الهاتف العادي"[2]. ولهذا فهو يشبه آلة التصوير الصغيرة، غير أنها متصلة بهاتف لإرسال الوثيقة ، فما على المرسل إلا أن يضعها في الجهاز، ثم يدير رقم هاتف جهاز فاكس المرسل إليه، وبمجرد أن يفتح الخط أو يتم الاتصال، تحرك الأداة الفاحصة الإلكترونية في جهاز الإرسال وتحول الصفحة المرسلة إلى مجموعة من الإشارات الكهربائية الرقمية التي تنتقل عبر خط الهاتف إلى جهاز فاكس المستقبل الذي يعيد الإشارات الكهربائية الرقمية مرة أخرى إلى نسخة طبق الأصل من الوثيقة الأصلية ثم يطبعها.

فالفاكس إذن، عبارة عن تقنية اتصال حديثة تشمل على:

1. جهاز استنساخ إلكتروني صغير مرتبط بخط الهاتف؛
2. جهاز هاتف مرتبط بخط هاتفي.

ويمكن تحديد أهم مميزات وخصائص الفاكس على النحو التالي:

- سهلة الاستخدام ولا تحتاج إلى خبرة أو فني متخصص؛
- رخيص الثمن ويمكن للأفراد شرائه؛
- لا يحتاج إلى متطلبات كثيرة، فخطوط الهاتف متوافرة في كل مكان؛
- مناسب جدا لنقل الوثائق والرسائل المالية والقانونية وكافة المطبوعات؛

[1] لمين علوطي ،مرجع سابق ، ص : 26-27 .

[2] محمد دياب مفتاح ، معجم مصطلحات نظم وتكنولوجيا المعلومات والاتصالات، الدار الجامعية للنشر، القاهرة، مصر، 1995، ص 63.

- من الصعب إرسال الوثائق عبر وسائل أخرى غير الفاكس بنفس السرعة والدقة والتكلفة؛
- يمكن إرسال الرسائل والوثائق إلى عدة جهات في نفس الوقت؛

- **الأقمار الصناعية [1]:**

بشكل عام، تصنف الاتصالات إلى نوعين رئيسيين هما:

أولا: الاتصالات الأرضية، سواء كانت سلكية أو لا سلكية.

ثانيا: الاتصالات الفضائية التي تتم عن طريق الأقمار الصناعية.

يعرف القمر الصناعي بأنه: "مركبة فضائية تدور حول الكرة الأرضية، لها أجهزة لنقل إشارات الراديو والبرق والهاتف والتلفزيون، وترسل محطات على سطح الأرض (المحطات الأرضية) الإشارات إلى القمر الصناعي الذي يبث الإشارات بعد ذلك إلى محطات أرضية أخرى، وجاءت فكرة الأقمار الصناعية معززة لطرق الاتصال عبر الأثير وكانت سعة الانتقال للدوائر الهاتفية التي تنقلها هذه الأقمار مغرية إلى حد كبير".[2]

ويتكون القمر الصناعي من:[3]

- أجهزة الاستلام والإرسال؛
- أجهزة التكبير والتضخيم؛
- جهاز تتبع الأرض؛
- محرك الاشتعال الرئيسي؛
- الهوائيات؛
- الخلايا الشمسية للطاقة؛
- جهاز تتبع الشمس؛
- محركات صاروخية جانبية؛
- خزانات الوقود.

وتقدم الأقمار الصناعية خدماتها لكونها محطات تحويل فضائية لبث إشارات ترسل بواسطة المحطات الأرضية والتي تعمل أيضا على ربط شبكات الاتصالات الأرضية من خلال شبكات الهاتف. وقد أخذت الاتصالات الفضائية عبر الأقمار الصناعية دورا هاما في مجال نقل

---

[1] لمين علوطي ،مرجع سابق ، ص :28-30

[2] الشافعي منصور، مملكة العلم والتكنولوجيا، ايتراك للنشر، مصر، 2000، ص 82.

[3] عامر ابراهيم قنديلجي ، ايمان فاضل السمرائي، مرجع سابق، ص : 230

الرسائل والمعلومات بفضل فعاليتها وعدم تأثرها بالظروف المحيطة. ويمكن القول أن للاتصالات عبر الأقمار الصناعية فائدتين هامتين هما:

أولا: إمكانية البث المتوافق، بحيث تستطيع كل محطة في الشبكة أن ترتبط مع كل المحطات الأخرى في نفس الوقت؛

ثانيا: إمكانية الوصول إلى أماكن بعيدة ودعمها للامركزية في أساليب جمع وتوزيع الرسائل والمعلومات.

وقد فتحت الأقمار الصناعية الباب على خدمات جديدة من بينها توفير نوع من الاتصالات بين الإنسان والآلة، وبين الآلة والأخرى كما تحدث في عملية الاتصال بين الحواسيب.

وتستخدم الأقمار الصناعية العديد من الوظائف والأنشطة والخدمات مثل نقل الصوت والصورة والبيانات والوثائق والمؤتمرات البعدية (**Teleconferencing**) والأرصاد الجوية، والاستشعار عن بعد، والبث التلفزيوني والخدمات الهاتفية وغيرها.

وتستطيع كذلك الأقمار الصناعية التعامل مع كمية ضخمة من البيانات وأن تنقلها بين الحواسيب وتستطيع تداول 30 ألف مكالمة هاتفية في وقت واحد، والوصول إلى جمع من الناس في وقت واحد[21].

ويمكن تحديد مجالات استخدام الأقمار الصناعية فيما يلي[2]:

1- الاتصالات الهاتفية، وتمتاز بأنها فورية ومباشرة وقليلة التكلفة- مقارنة مع الوسائل الأخرى- كما أنها خالية من التشويش والاضطراب الذي يحدث في الاتصالات الأرضية.

2- النقل التلفزيوني المباشر للبرامج المختلفة؛

3- خدمات تجارية للطائرات والملاحة الجوية والبحرية والأرصاد الجوية وغيرها؛

4- نقل المعلومات والخدمات الأخرى بين الدول؛

5- التنقيب عن الثروات الطبيعية كالنفط والمعادن وغيرها...؛

6- الأغراض العسكرية مثل رصد التحركات العسكرية والتجسس.

وتعد الأقمار الصناعية وسيلة اتصال فضائية متقدمة تميز عن غيرها من وسائل الاتصال (السلكية ولا سلكية) بالمميزات التالية:

---

[1] عامر ابراهيم قنديلجي ، ايمان فاضل السمرائي، مرجع سابق، ص ص : 232-233

- قدرتها على نقل المعلومات وتوفير الترابط على المستوى العالمي بكفاءة عالية؛
- ملائمة ومثالية لتناقل وتناول جميع أشكال الربط بين الشبكات القياسية التشابهية (Analog) والرقمية (Digital)؛
- توفر الوصول المتزامن (في نفس الوقت) من وإلى العديد من النقاط الموزعة في دول العالم؛
- إمكانية بناء شبكات إقليمية للاتصالات والمعلومات أو توسيعها أو إعادة بناء هيكلها. سواء كانت هذه الشبكات واسعة أو محددة؛
- قادرة على تسهيل وتوفير الوصول إلى شبكات الاتصال القريبة من المستفيدين وتقليص تكاليف ونفقات الاتصال؛
- الاتصال عبر الأقمار الصناعية يؤمن نقل المعلومات بأشكالها المختلفة مثل: النصوص، الأرقام و الرسومات والأشكال، الأصوات الموسيقى الصور، وغير ذلك من الأوعية والوسائط؛
- كمية وحجم المعلومات المنقولة في الثانية الواحدة عن طريق الأقمار الصناعية أكبر بكثير من أية وسيلة أخرى من وسائل الاتصال المستخدمة حاليا.

وفي نهاية المطاف سادت نظم كوابل الألياف الضوئية[1] بعد إشراكها في صراع محموم مع أنظمة الاتصالات عبر الأقمار الصناعية، فهي تمتع بارتفاع في سعة النقل وانخفاض كلفتها وطول عمرها

وحاليا تطورت هذه التكنولوجيا الى كل من المحاضرات المرئية الحانية و الفيديو كونفيرونس والمحاضرات السمعية بالإضافة إلى خدمات الدردشة و المتصفحين .

أما فيما يخص البريد الإلكتروني و مجموعات التحاور الإلكتروني و الشبكات الداخلية فسوف نتناولها لا حقا .

ثانيا : الشبكات المعلوماتية

قبل التطرق إلى المفاهيم الأساسية لهذا المطلب يجب أولا التعرف على الوسائل التي تعد أساس هذه الشبكات و المتمثلة في الحاسوب (الكمبيوتر) و البرمجيات :

1-الحاسوب و البرمجيات : و سنتطرق للأول بشيء من التفصيل.

- **الحاسوب** : يعرف الحاسوب بأنه: "آلة الكترونية أوتوماتيكية لمعالجة المعلومات بمختلف أنواعها ويستطيع حفظها و استرجاعها كليا أو جزئيا عند الطلب "[39]

[1]إبراهيم بختي، تكنولوجيا ونظم المعلومات في المؤسسات الصغيرة والمتوسطة، المرجع السابق.

كما انه :" آلة تقوم بأداء العمليات الحسابية والمنطقية على البيانات الرقمية بوسائل الكترونية و تحت تحكم البرامج المخزنة به"[1]

من خلال التعريفين المقدمين يتضح انه يتميز بمجموعة من الخصائص يمكن إدراجها فيما يلي :

- الدقة في أداء العمليات؛
- السرعة العالية التي تساعد على توفير الوقت في أداء العمليات؛
- المرونة في تأدية العديد من الأعمال وعدم الاقتصار على أداء عمل واحد فقط؛
- السعة الكبيرة في تخزين البيانات والسرعة في استرجاعها عند الطلب؛
- قابلية التوسع والنمو في ذاكرته الأصلية والذاكرات الثانوية التي تلحق به، وإضافة ملحقات مساعدة.

- **تطوره :**[2] و قد تطور عبر مراحل يمكن تلخيصها في ما يلي :

- **الجيل الأول 1946-1959 :** ظهر هذا الجيل بجامعة **Pennsylvanie** مابين 1944-1946 من خلال أعمال Mouchly وEckert على شكل أول آلة الكترونية تحتل مساحة تقارب 160م،وكانت تعمل بالصمامات المفرغة و تستهلك الكثير من الطاقة و تفرز الكثير من الحرارة.
- **الجيل الثاني 1959-1965:** و قد استعمل في هذا الجيل الترانزستور بدلا من الصمامات المفرغة و التي ساعدت على التغلب على مشكلة الحرارة و أقلة من معدلات التوقف و وفرت في الطاقة .
- **الجيل الثالث 1964-1970:** و الفروق بينه و بين الجيل الذي يسبقه هي :
  - صغر حجمه ،و الذي نتج عن استعمال الالكترونيات الدقيقة بإدماج الدوائر الالكترونية
  - تطور الذاكرات الفرعية القادرة على استيعاب معلومات كبيرة بأقل تكلفة
  - تطور لغات البرمجة مثل ظهور البازيك و الباسكال .
- **الجيل الرابع من بداية 1970:** و قد ارتبط باكتشاف و تطوير**Micro-processors** و الذي يعتمد على تقنية دمج أكبر عدد ممكن من المكونات الأساسية على شريحة واحدة

[1] مراد رايس ، مرجع سابق ، ص: 33

[2] محمد صالح الحناوي و آخرون ، نظم و تكنولوجيا المعلومات في الاعمال في عصر التكنولوجيا، ، الدار الجامعية، الإسكندرية، مصر، 2004 ص ص :296-298

، كما تم التوصل لصناعة الذاكرات المعتمدة على شرائح السيلكون ذات الحجم الصغير و السعة الكبيرة .

- **الجيل الخامس من الآن إلى المستقبل** : و هو جيل قيد التحضير و هو محور بحوث تجرى في اوروبا و الولايات المتحدة و اليابان حيث تعمل هذه الدول على ابتكار ما يسمى بالحواسيب الذكية و التي يمكنها القيام بكثير من الأعمال المكتبية

من خلال إدماج اللغة العادية كتابيا و التواصل الصوتي مع الآلة .

- **البرمجيات** : يعد هذا العنصر من مركبات تكنولوجيا المعلومات بمثابة الروح و الجسد ، فدونها لا يمكن الاستفادة من العتاد التكنولوجي ، فهي بذلك تعد حلقة الوصل بين المستخدم و الآلة أي أنها برامج تساعد على حفظ المعلومات بنظام ، و يمكن تعريفها بأنها: "مجموعة منفصلة من التعليمات و الأوامر المعقدة و التي توجه المكونات المادية للحاسوب للعمل بطريقة معينة بغرض الحصول على النتائج المطلوبة "[1].

و للبرمجيات لغات عدة تشكل وسيلة تخاطب الإنسان مع الآلة تنقسم إلى :

- **لغات متدنية الأداء** : و تشمل :
  - لغة الآلة : و هي اللغة الوحيدة التي يفهمها الحاسوب و قد استخدمت في كتابة برمجيات الجيل الأول منه.
  - لغات التجميع: وهي ناتجة عن صعوبة كتابة البرامج بلغة الآلة فهي بذلك تشكل تطويرا لها لتجاوز تلك الصعوبة.
- **لغات المستوى العالي** : مثل بيسيك ،كوبول ، باسكال .
- **لغات الجيل الرابع** : مثل دي بيس ، اورا كل.

2- مفهوم الشبكات المعلوماتية :

- **شبكة الانترنت :**

هي تجميع لشبكات متصلة فيما بينها لتشكل بذلك عالمية اكبر "[2] .

و بذلك فهي تتصف بمجموعة من الخصائص تميزها عن باقي الشبكات يمكن تلخيصها كما يلي [3]:

---

[1] عامر إبراهيم قنديلجي ، ايمان فاضل السمرائي ، مرجع سابق ، ص 160

[2] مراد رايس ، مرجع سابق ، ص 44 .

[3] هشام بن عبد الله عباس ، المكتبات في عصر الانترنت تحديات و مواجهات ، مجلة العربية 3000، العدد2،2001، ص ص:296-298

° **مفتوحة ماديا ومعنوية** : أي يمكن لأي شبكة أن ترتبط بها .

* **عملاقة و متنامية** : أي أنها حققت ما لم تحققه أي تقنية سابقة من حيث السرعة و الابتكار و النمو
* **العشوائية** : أي أن المعلومات تتواجد فيها بشكل متناثر مما دفع بعدة جهات إلى إنشاء فهارس و تطوير برامج للبحث ، كما يصعب الرقابة عليها أو محاسبة من ينشر فيها .
* **الشعبية** : فلا توجد وسيلة حاليا تضاهي شعبيتها و هي ليست مقصورة على عن جهة معينة .
* **وسيلة للتجارة الالكترونية** : فهي تعد وسيلة تجارية و تسويقية فعالة مقارنة مع الوسائل الأخرى .
* **متطورة باستمرار**: ساهمت البحوث المنجزة في تكنولوجيا المعلومات في تطورها المستمر و نموها نحو الأحسن .

المبحث الثاني: الجرائم الماسة بتكنولوجيات الاعلام والاتصال وتقنية المعلومات ومكافحتها.

المطلب الأول: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1]

يشهد العالم العربي جملة من التحديات في موجة شرسة من الاختراقات في انظمة الحواسيب وفي أكبر مفاصل وهياكل الدولة، وهذا ما يبرهن أن هناك سلطة عليا تتحكم في تقنية المعلومات، وكان لهذه الدول أن قامت بتصنيف هذه الافعال بالجرائم الماسة بالدولة والتي تمس تكنولوجيا المعلومات والاتصالات المختلفة.

لاشك أن الدول العربية قد ضاقت مرارة هذه الجرائم وأحست بخطرها الوشيك، فجعلت على عاتقها مسؤولية الوقاية منها ومكافحتها بشتى الوسائل، فكان ولابد من توحيد الجهود وجمع شمل الدول المتضررة من ارهاب المعلوماتية في صف واحد نظرا لوجود الخطر واحد، وقد تمخض عن ذلك ميلاد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 2010/12/21.

كان الهدف من انشاء هذه الاتفاقية العربية هو تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، حفاظا على أمن هذه الدول ومصالحها وسلامة المجتمع

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21 والتي صادقت عليها الجزائر بالمرسوم الرئاسي 252/14 المؤرخ في 2014/09/08 (ج ر 57 بتاريخ 2014/09/28).

والافراد. لذلك كان مبدا التجريم هو أساس الاتفاقية والتزام كل دولة عربية به بوضعه ضمن منظومتها التشريعية الداخلية.

الفرع الأول: الجرائم المرتبطة بتقنية المعلومات

هي تلك الجرائم التي توجه بصفة اساسية لتقنية المعلومات بالمعنى السابق تحديده، والتي تشمل الجرائم الموجهة للمواقع والبرامج والانظمة المعلوماتية او الالكترونية، أو احدى وسائل تقنية المعلومات، ومن ثم لا نتصور ارتكابها دون استخدام وسيلة تقنية المعلومات، حيث تقع على احدى وسائل تقنية المعلومات او من خلال موقع الكتروني او شبكة معلوماتية. فهي جرائم يعد من اركانها، أو من العناصر الاساسية المكونة لاحد اركانها، وسيلة تقنية المعلومات، هذه الجرائم من الصعب تصور حدوثها دون أن تكون وسيلتها او محلها او نتيجتها متصلة بتقنية المعلومات[1].

وقد تضمنت الاتفاقيات الاقليمية المتعلقة بجرائم تقنية المعلومات مثل الاتفاقية الاوروبية والاتفاقية العربية ووثيقة الرياض للقانون الموحد، وكذلك تشريعات مكافحة الجرائم المعلوماتية مثل هذا النوع من الجرائم.

وأغلب هذه الجرائم في التشريعات العربية تتعلق بالدخول غير المشروع واعاقة الوصول الى الشبكة المعلوماتية أو الاعتراض غير المشروع والاعتداء على سلامة البيانات واساءة استخدام وسائل تقنية المعلومات وجريمة الاعتداء على حرمة الحياة الخاصة وغيرها من الجرائم.

ويتميز الجرم المعلوماتي بعدة خصائص تميزه عن غيره من الجرائم الاخرى، ويمكن تلخيص هذه الخصائص بما يأتي:

- تكرار الفاعل للجريمة المعلوماتية: يعود العديد من المجرمين في تقنية المعلومات الى تكرار ارتكاب هذا النوع من الجرائم المستحدثة إما لاهتمامهم بالاطلاع على المعلومات وكشف

[1] أ.د. إمام حسنين عطاالله، جرائم تقنية المعلوماتية التشريعات والصكوك العربية، دار جامعة نايف للنشر، الرياض، 2017، ص142.

الاسرار، او حصولهم على الارباح المالية جزاء ارتكاب هذه الجرائم، أو اضرارا بالغير[1]، أو لاظهار تفوقه على الالة أو بدافع اللهو والترف[2].

- تخصص الفاعل المجرم في تقنية المعلوماتية: يعد المجرمين الذين يمتازون بالتخصص في تكنولوجيات المعلومات، حيث يكتسب قدرة ذهنية وعقلية تمكنه من التعامل مع الاجهزة والانظمة الخاصة بتكنولوجيات الاتصال والاعلام في ارتكاب الجرائم المعلوماتية بسهولة وسرعة عالية وفي وقت قصير[3].

سوف نعرض لطوائف بعض الجرائم وفق ما جاء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أولا: جريمة الدخول غير المشروع

احتلت جرائم الدخول غير المشروع لوسائل تقنية والمعلوماتية أهمية قصوى في التشريعات العربية، فلا يكاد يخلو تشريع من تجريم أعمال الدخول غير المشروع أو مقدمات هذا الدخول، أو ما يترتب على الدخول من اثار اهمها التاثير على البيانات، بل أن بعض التشريعات تحرص على وضع تعريف للدخول غير المشروع في صدر مواد التشريع مثل النظام السعودي لمكافحة الجرائم المعلوماتية وقانون مكافحة جرائم تقنية المعلومات الكويتي[4].

وتتضمن التشريعات الوطنية أسوة بالاتفاقيات الأقليمية بشأن مكافحة جرائم تقنية المعلومات، تجريم مجموعة من الافعال التي تمثل دخولا غير مشروع للشبكة المعلوماتية أو نظم المعلومات او البرامج، وهي تجرم الدخول المجرد في ذاته مادام عمديا وبدون تصريح، وتتعود صور الدخول غير المشروع بالنظر الى صفة مرتكب الجريمة او طبيعة البيانات التي اطلع عليها، او ينوي

---

[1] د. نظام توفيق المجالي، شرح قانون العقوبات، ط2، دار الثقافة للنشر والتوزيع، عمان، 2010، ص225.

د. لورنس سعيد الحوامدة، الجرائم المعلوماتية، اركانها والية مكافحتها، دراسة تحليلية مقارنة، مجلة الميزان للدراسات الاسلامية القانونية، جامعة العلوم الاسلامية، المملكة العربية السعودية، 2017، ص13.

[2] هلال بن محمد بن حارب البورسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة، 2009، ص 35.

[3] د. هدى حامد قشقوش، جرائم الحاسب الالي في التشريع المقارن، ط1، دار النهضة العربية، القاهرة، 1992، ص27.

[4] أ.د. إمام حسنين عطاالله، جرائم تقنية المعلوماتية التشريعات والصكوك العربية، المرجع السابق، ص140.

أن يطلع عليها من قام بالدخول، أو طبيعة الاضرار التي اصابت وسيلة تقنية المعلومات جراء هذا الدخول أو ما ينوي الجاني عليه بها[1].

1- الأساس القانوني لجريمة الدخول غير المشروع

تتكون كل جريمة من هذه الجرائم من ركنين: أحدهما مادي، يتمثل في فعل الدخول ذاته، والاخر معنوي يتمثل في القصد الجنائي، والقائم على العلم والارادة، وقد تطلبت الاتفاقية الاوروبية أن يكون الدخول عمداً وبغير حق، وسواء كان ذلك لقصد الحصول على بيانات الكمبيوتر أو بقصد اخر غير آمن.

كما تطلبت ايضا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من كل دولة تجريم الدخول أو البقاء وكل اتصال غير مشروع مع تقنية المعلومات كاملة أو جزء منها، أو الاستمرار بها[2]، وشددت العقوبات إذا ترتب على الدخول أو البقاء أو الاستمرار بهذا الاتصال أي تأثير على البيانات المحفوظة أو الاجهزة أو الانظمة أو الحاق الضرر بالمستخدمين والمستفيدين أو ترتب على ذلك الحصول على معلومات حكومية سرية[3].

2- المقصود بجريمة الدخول غير المشروع

المقصود بهذه الجريمة أن يتم قيام أي شخص أو هيئة بالدخول، أو البقاء أو الاتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

ومن مظاهر هذه الأعمال غير المشروعة والتي تشدد فيها العقوبة إذا ترتب على الدخول أو البقاء أو الاتصال محو او تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللاجهزة والانظمة الالكترونية وشبكات الاتصال والحاق الضرر بالمستخدمين والمستفيدين. أو الحصول على معلومات حكومية سرية[4].

3- أركان جريمة الدخول غير المشروع

سوف نعرض لأركان هذه الجريمة من خلال تناول ركنيها المادي والمعنوي، وذلك على النحو التالي[5]:

---

[1] أ.د. إمام حسنين عطاالله، جرائم تقنية المعلوماتية التشريعات والصكوك العربية، المرجع أعلاه، ص141.

[2] م2/6 من نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والوقاية منها لسنة 2010 المشار اليها سابقا.

[3] م2/6 ب من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والوقاية منها لسنة 2010 المشار اليها أعلاه.

[4] م 6 من الاتفاقية المشار اليها أعلاه.

[5] أ.د. إمام حسنين عطاالله، جرائم تقنية المعلوماتية التشريعات والصكوك العربية، المرجع السابق، ص144.

أ- الركن المادي: كان هذا الركن محل دراسة من طرف كل التشريعات العربية، وقد جرمت الاتفاقية العربية لسنة 2010 ثلاث صور لهذه الجرائم هي: الدخول بدون تصريح، تجاوز حدود التصريح، والبقاء بصورة غير مشروعة.

وعليه سنقوم بعرض صور السلوك الاجرامي في جريمة الدخول غير المشروع، والتي يكفي أي صورة منها لقيام هذا السلوك، وذلك على النحو التالي: الدخول دون تصريح: يتطلب الدخول هنا الحصول على إذن أو تصريح مسبق، وقد يكون الاذن او التصريح صريحا أو ضمنيا، مكتوبا أو شفهياً.

- **تجاوز حدود التصريح:** يتمثل التجاوز لحدود التصريح الدخول على بيانات أخرى أو تجاوز نوعية البيانات المصرح له بالاطلاع عليها، وبهذا يكون مرتكبا للجريمة في صورتها التامة.
- **البقاء بصورة غير مشروعة:** هو التواجد بصورة غير مشروعة داخل نظام المعالجة الالية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام.
- **محل الدخول غير المشروع:** مع اختلاف التشريعات العربية فان الدخول غير الشروع لابد أن يكون الى أي من المواقع الالكترونية، او نظام المعلومات الالكتروني، او شبكة معلومات، او وسيلة تقنية معلومات، وقد اقتصر بعض القوانين العربية كالمشرع البحريني مثلا على ان يكون الدخول غير المشروع على نظام تقنية المعلومات أو جزء منها.

ب- الركن المعنوي

جرائم الدخول غير المشروع – بصورها الثلاث- هي جرائم عمدية تقع بطريق الخطأ، ومن ثم فالركن المعنوي فيها هو القصد الجنائي، الذي يتكون من العلم والارادة، فلابد أن ينصرف علم الجاني الى العناصر الاساسية للجريمة، مثل علمه بالموقع الالكتروني، او نظام المعلومات الالكتروني او شبكة المعلومات أو وسيلة تقنية المعلومات، وجميعها تعد محل للنشاط الاجرامي، والتي يجب أن ينصرف اليها علم الجاني، وإذا كان الجاني يعتقد أنه لا يدخل الى نظام معلوماتي أو موقع الكتروني فإن هذا ينفي لديه القصد الجنائي باعتبار أن الموقع الالكتروني او النظام المعلوماتي عنصر لازم للتجريم لأنه محل السلوك الاجرامي[1].

ثانيا: جريمة الاعتراض غير المشروع

هذه الجريمة تتمثل في القيام باعتراض متعمد وغير مشروع لمسار البيانات المخطط لها وذلك بأي وسيلة من الوسائل الفنية، وقطع بث أو استقبال بيانات تقنية المعلومات.

[1] إمام حسنين عطاالله، جرائم تقنية المعلوماتية التشريعات والصكوك العربية، المرجع السابق، ص151.

ثالثا: الاعتداء على سلامة البيانات

هذه الجريمة مفادها قيام شخص بتدمير أو محو أو اعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصداً وبدون وجه حق. ويكون هذا الشخص مجرما بهذا الفعل إذا تسبب في ضرر جسيم.

رابعاً: جريمة إساءة استخدام وسائل تقنية المعلومات

تنحصر هذه الجريمة في كل الافعال التي تتم في اطار تقنية المعلومات من انتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير لأية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المشار اليها سابقاً. او القيام بهذه الاعمال باستعمال كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المشار اليها مقدماً.

كما تعد ايضا جريمة اساءة استخدام وسائل تقنية المعلومات إذا ما تمت حيازة أية أدوات او برامج المذكورة سابقا بقصد استخدامها لغايات ارتكاب أي من الجرائم المشار اليها انفا.

خامساً: جريمة التزوير

هذه الجريمة تتعلق بقيام الجاني باستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

سادساً: جريمة الاحتيال

هي جريمة تتعلق بالقيام بالطرق الاحتيالية لتحقيق المصالح والمنافع بطريقة غير مشروعة لفائدة المحتال أو الغير، عن طريق ادخال أو تعديل أو محو أو حجب المعلومات والبيانات، التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها. وكذا تعطيل الاجهزة والبرامج والمواقع الالكترونية.

ويشترط في توفر أركان هذه الجريمة أن يقصد من وراء الاحتيال الحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق وبنية الاحتيال.

سابعاً: جريمة الاباحية

تعتبر هذه الجريمة من أقوى واكثر الجرائم شيوعاً، حيث تتمثل يتم من خلالها استعمال تقنية المعلومات في انتاج وعرض او توزيع او توفير او نشر او شراء او بيع او استيراد مواد اباحية او مخلة بالحياء، وتشدد العقوبة إذا ما تمت الجريمة من قبل الاطفال والقصر بحيازة مواد اباحية او مواد مخلة بالحياء على تقنية المعلومات او وسيط تخزين تلك التقنيات.

كما تعتبر المغامرة والاستغلال الجنسي ايضا من الجرائم المرتبطة بالاباحية[1] .

ثامناً: جريمة الاعتداء على حرمة الحياة الخاصة

إن الحياة الخاصة للإنسان تشمل الحق في العيش مع ذاته و أسرته في هدوء وسكينة، والحق في السرية المهنية ، وسرية المراسلات والمحادثات، حرمة المساكن وحرية الاعتقاد والفكر، المسألة العاطفية والعائلية، والروحية والمالية ..الخ ، وهي من المظاهر الاجتماعية الضرورية لكل إنسان. وجزءاً لا يتجزأ من الوجود الإنساني تجب حمايته بكل قوة من التعسف والاعتداء أ ياً كان الشخص المعتدي وبغض النظر عن المعتدى عليه أو الوسيلة المستعملة في الاعتداء[2].

ولتكييف فعل الاعتداء يمكن أن نعتمد على طبيعة الحق المراد حمايته، أي الحق في الحياة الخاصة، هذه الأخيرة التي تشمل كل الحقوق الشخصية أو اللصيقة بالشخصية التي تهدف الى حماية الكيان الأدبي للإنسان، الأمر الذي يجعلنا نكيف هذه الحقوق بالأدبية، لكن بالنظر إلى جسامة الأضرار في بعض جرائم المعلوماتية التي تمس الحياة الخاصة فهي جريمة يعاقب عليها قانون العقوبات إعمالا لنص المادة 394 مكرر 2 من القانون رقم 15/04 و التي تنص على أنه" :يعاقب...كل من يقوم عمدا وعن طريق الغش بما يأتي :

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. "

نظم المشرع الجزائري حماية الحق في الحياة الخاصة من كل أشكال الاعتداءات التي يمكن أن تتعرض لها مهما كانت الوسيلة المستعملة في إلحاق الضرر بالشخص، حيث كيف هذه الاعتداءات بالجنحة فيؤسس الحق في الحماية الجزائية بمجرد توافر أركان الجريمة كقاعدة عامة، وقد وردت العقوبات في قوانين مختلفة، وسمح باللجوء إلى القواعد العامة للاستفادة من الحماية المدنية بموجب تأسيس الدعوى على المسؤولية التقصيرية أو المدنية إذا تعذر أو إذا لم تكتمل أر كان الجنحة .

---

[1] م 13 من الاتفاقية العربية المشار اليها سابقا.

[2] المحامي يونس عرب المصدر: http://www.arab-elaw.com/show_similar.aspx?id=20

حاول المشرع الجزائري أن يتماشى مع ما هو معمول به في مجال محاربة الإجرام الاليكتروني باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية، بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات خاصة بسبب التزايد اللا متناهي للاعتداءات على الأنظمة المعلوماتية بتطور آليات الاتصال وظهور مواقع الاليكترونية والانترنت .و قد نصت المادة 303مكرر من قانون العقوبات المعدل بالقانون رقم 06-23المؤرخ في 2006/12/20 [22]على ما يلي" :يعاقب بالحبس من ستة أشهر إلى 3سنوات كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص ، بأي تقنية كانت و ذلك :

-1التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية ، بغير إذن صاحبها أو رضاه

-2التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص ، بغير إذن صاحبها أو رضاه."

ويعاقب على الشروع في ارتكاب نفس الجنحة بالعقوبات ذاتها المقررة للجريمة التامة. وتضيف المادة 303 مكرر1 ما يلي" : يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة .وتصادر كالأشياء التي تستعمل لارتكاب الجريمة بل وتغلق حتى المواقع التي تتم فيها الاعتداءات بل وحتى المحلات التي وقعت فيها الجريمة إذا تمت بعلم صاحبها.

وتضمن القانون رقم 15/04 المؤرخ في 2004/11/10 ، المتضمن تعديل قانون العقوبات، تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، حيث نصت المادة 394 مكرر منهما يلي" :يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة" تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000إلى 150000دج[23]."و ذلك مهما كانت قاعة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة. ونصت المادة 394 مكرر 2 على أنه" :يعاقب...كل من يقوم عمدا و عن طريق الغش بما يأتي :

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. "

وتضيف المادة 394 مكرر6 أنه بالإضافة إلى العقوبات الأصلية أي الحبس و الغرامة وبالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية:"يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلاً لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه".

تاسعا: الجرائم المتعلقة بالارهاب والمرتكبة بواسطة تقنية المعلومات.

تمثل هذه الجرائم في مايلي:- نشر افكار ومبادئ جماعات ارهابية والدعوة لها، - تمويل العمليات الارهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الارهابية.- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات ارهابية.- نشر النعرات والفتن والاعتداء على الاديان والمعتقدات.

عاشرا: الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات

تنحصر هذه الجرائم في القيام بعمليات غسيل أموال أو طلب المساعدة او نشر طرق القيام بغسل الاموال والترويج للمخدرات والمؤثرات العقلية او الاتجار بها، الاتجار بالأشخاص، الاتجار بالأعضاء البشرية والاتجار غير المشروع بالأسلحة.

احدى عشر: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة

تتم هذه الجريمة بانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة، اذا تم ارتكاب الفعل عن قصد ولغير الاستعمال الشخصي.

اثنى عشر: الاستخدام غير المشروع لأدوات الدفع الالكترونية

تمثل هذه الجريمة في القيام بتزوير او اصطناع أو وضع أي اجهزة او مواد تساعد على تزوير او تقليد أي اداة من ادوات الدفع الالكترونية باي وسيلة كانت. وايضا القيام بالاستيلاء على بيانات أي اداة من ادوات الدفع واستعمالها او تقديمها للغير أو تسهيل للغير الحصول عليها. الاستخدام الشبكة المعلوماتية او احدى وسائل تقنية المعلومات في الوصول بدون وجه حق الى ارقام او بيانات أي اداة من ادوات الدفع. قبول أداة من ادوات الدفع المزورة مع العلم بذلك.

المطلب الثاني: قانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

المشرع الجزائري حينما أصدر القانون 04/09 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها خالف الاتفاقية العربية لمكافحة تقنية المعلومات فيما يتعلق بالمصطلح، حيث نجد هناك فرق شاسع بين تكنولوجيات الاعلام والاتصال وبين تقنية المعلومات[1]، فهذه الاخيرة لها مفهوم عام واشمل ليدخل ضمنها الكثير من الدلالات التي تعني المعلوماتي.

ويقصد بها تلك الوسائل المادية والمعنوية المستعملة لتخزين المعلومات واستعمالها بعد ذلك عن طريق جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكيا في نظام أو شبكة. أما تكنولوجيات الاعلام والاتصال فلها مفهوم ضيق يحصر في الاتصال والاعلام الالكترونين، فهي أنظمة المعالجة الالية للمعطيات ومنظومات المعلوماتية أو نظام للاتصالات الالكترونية. ولعل المقصود بهذا الاختلاف أن منظومة تكنولوجيات الاعلام والاتصال تحكم فيها الدول ممثلة بوزارة البريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة، أما تقنية المعلومات فهو مفهوم عام يمارس من قبل أي جهاز مرخص به من طرف دولة ما.

الفرع الأول: الجرائم المرتبطة بتكنولوجيات الاتصال والاعلام

جاء القانون 04/09 بهدف الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ويقدم اليات مراقبة الاتصالات الالكترونية وتجميعها وتسجيلها من أجل القيام باجراءات التفتيش والحجز داخل منظومة معلوماتي.

اولا: مراقبة الاتصالات الالكترونية

سمح القانون باجراء مراقبة للاتصالات الالكترونية وفقط وليس غيرها من الانظمة التي جاءت بها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لذلك فهناك فرق بين الرقابة والمراقبة، فالرقابة هي المتابعة عن بعد والمحافظة على تطبيق القانون في مجال معين، اما المراقبة فتفيد الاستمرار والتتبع غير المنقطع لمعرفة ما يجري داخل ميدان معين. ومن ثم فان المشرع الجزائري لم يترك المراقبة على اطلاقها بل حدد عمليات المراقبة لتشمل ثلاث حالات فقط[2]:

---

[1] طالع المادة 2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمادة 2 ايضا من القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها(ج ر 47 بتاريخ 2009/16.08).

[2] م 4 من القانون 04/09 المشار اليه.

- المراقبة من أجل الوقاية من الافعال الموصوفة بجرائم الارهاب او التخريب او الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الابحاث الجارية دون اللجوء الى المراقبة الالكترونية.
- في اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

للإشارة فانه يمنع قانونا على اللجنة المكلفة بالمراقبة استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة الا في الحدود الضرورية للتحريات او التحقيقات القضائية[1].

ثانيا: اجراءات القضائية لتنفيذ المراقبة

1-الاذن العام بالمراقبة: لا يجوز القيام بإجراء الرقابة الا باذن مكتوب من السلطة القضائية المختصة،

2- الاذن الخاص بالمراقبة: يتعلق الأمر بالافعال الموصوفة بجرائم الارهاب او التخريب او الجرائم الماسة بأمن الدولة، الذي يختص به النائب العام لدى مجلس قضاء الجزائر، حيث يمنح لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته إذناً لمدة ستة(06) اشهر قابلة للتجديد وذلك على اساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والاغراض الموجهة لها.

المقصود بهذه الترتيبات والاغراض هي التي تكون موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الافعال الارهابية والاعتداءات على امن الدولة ومكافحتها. مع مراعاة العقوبات الخاصة بالنسبة للمساس بالحياة الخاصة للغير[2].

ثالثا: تفتيش للمنظومات المعلوماتية

1- اجراءات التفتيش

اجاز القانون للسلطات القضائية المختصة وضباط الشرطة القضائية الدخول للمنظومات المعلوماتية أو جزء منها والى المعطيات المعلوماتية المخزنة فيها وايضا داخل منظومة تخزين معلوماتية بغرض التفتيش ولو عن بعد.

---

[1] م 9 من ق 04/09 المشار اليه انفا.

[2] فقرة أخيرة من م 4 من القانون 04/09 اعلاه.

كما يجوز تمديد التفتيش شريطة الاعلام المسبق للسلطة القضائية المختصة إذا كان هناك سببا داع لذلك كالاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية اخرى وان هذه المعطيات يمكن الدخول اليها انطلاقا من المنظومة الأولى، واذا كانت هذه المعلومة المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الوطن فيمكن الاستعانة بالسلطات الاجنبية المختصة طبقا للاتفاقيات الدولية ووفقا لمبدا المعاملة بالمثل.

ويمكن الاستعانة باي شخص له دراية بعمل المنظومة المعلوماتية محل البحث قصد تقديم المساعدة والتزود بكل المعلومات الضرورية لانجاز مهمة اللجنة المكلفة بالتفتيش[1].

2- حجز المعطيات المعلوماتية

تقوم لجنة التفتيش بدور مهم في البحث والتحري على المعطيات المعلوماتية، فكلما اكتشفت بان هناك معطيات مخزنة اثناء التفتيش في منظومة معلوماتية وكان ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز. كما يحق لهذه اللجنة ان تتعامل مع هذه المعطيات بالوسائل التقنية الضرورية لتشكيلها او اعادة تشكيلها قصد جعلها قابلة للاستغلال لأغراض التحقيق، بشرط أن لا يؤدي ذلك الى المساس بمحتوى المعطيات[2].

كما يجب على لجنة التفتيش والحجز السهر على سلامة المعطيات التي هي محل البحث[3].

3- الحجز عن طريق منع الوصول الى المعطيات

يمكن للجنة المكلفة بالقيام باجراءات الحجز والتي استحال عليها هذا الاجراء لاسباب تقنية أن تقوم باستعمال تقنيات او نسخ المعطيات لمنع وصول الاشخاص الذين تحت تصرفهم هذه المعطيات والمرخص لهم باستعمال هذه المنظومة[4].

ويمكن لها ايضا ان تتخذ اي اجراء لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة[5].

الفرع الثاني: اللجنة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته

---

[1] م 5 من القانون 04/09 المذكور اعلاه.

[2] م 6 من ق 04/09

[3] فقرة " من م 6 من ق 02/09 أعلاه.

[4] م 7 من ق 04/09

[5] م 8 من ق 04/09.

تعتبر هذه اللجنة التي تم انشاؤها بموجب القانون 04/09 هيئة وطنية تشرف على الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته، وتتولى بالخصوص المهام التالية:

- تنشيط وتنسيق عمليات الوقاية من هذه الجرائم.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات الخاصة بهذه الجرائم بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذه الجرائم وتحديد مكان تواجدهم.

الخاتمة:

تعد تكنولوجيا المعلومات العصب المحرك لأي دولة بما تقوم به من حركية وتنظيم داخل هياكلها اختلاف مجالاته، كما إنها أصبحت الطفرة الاساسية والقيمة المضافة التنافسية التي تتمتع بها أي مؤسسة، وفي الحقيقة العبرة ليست بوجود هذه التقنية رغم ان ذلك مهم جداً، لكن في توفر مقومات استثمارها ولا تقتصر مقومات الاستثمار على الجوانب التنظيمية فحسب وإنما تشمل كل الجوانب القانونية واليات مكافحة الجرائم المتصلة بالمعلوماتية.

إن نجاح نظام المعلوماتية في الاتصال والاعلام يتوقف على مدى فعلية هذا الاتصال وكفاءته إذن فهما وجهان لعملة واحدة.

لقد حولت ثورة المعلومات المعرفة إلى مورد أساسي من الموارد الاقتصادية، وذلك أصبح تكنولوجيا المعلومات والاتصال أحد عوامل الإنتاج إذ أنها تزيد في الإنتاجية وفرص العمل كما أن تقنية المعلومات أصبح لآن قاطرة التنمية والتطور الاقتصادي العالمي.

كما تمثل تكنولوجيا المعلومات والاتصالات لو أحسن استغلالها فرص تمية للإسراع بجهود التنمية المجتمعية الشاملة والمستدامة بالوطن العربي عموما والجزائر خصوصا والذي لا ينقصه الموارد التي تؤهله لتبوء موقع متميز له على الخريطة الجيومعلوماتية وتقليص الفجوة الرقمية التي تفصل بينه وبين العالم وما بين البلدان العربية وفي داخل هذه االدول.

ان الخلاصة التي يمكن التوصل اليها من خلال هذا البحث هي ان تقنية المعلومات تعتبر المسألة الحاسمة في تمكين المجتمع العربي من توسيع مجالات اختياراتهم وتحقيق طموحاتهم، وتمثل تكنولوجيا المعلومات والاتصالات الادوات الاساسية للمجتمعات التي تنشد التقدم المؤسس على الاقتصاد المعرفي المرتكز الاساسي للتحول الحقيقي نحو استغلال الموارد الطبيعية والمادية، وبالتالي التأسيس لبعد جوهري في التنمية البشرية.

وقد توصل البحث الى جملة من الاستنتاجات ، اهمها :

1- غياب التبادل الافقي في مجال المعلومات بين البلدان العربية بسبب ضعف البنى التحتية، هجرة الموارد البشرية العربية، بالاضافة الى محدودية حجم الاسواق العربية وعدم استقرارها في اجتذاب رؤوس الاموال

2- هناك فجوة بين مجوعة الدول العربية المجتمعات الانسانية الأخرى في العالم على صعيد الخبرة الادارية للمعلومات والخبرة الفنية وكذلك في مجال القوانين والانظمة المتعلقة بالتطور التكنولوجي الحديث.

3- جمود التشريعات والانظمة والقوانين وعدم مسايرتها للتطور المعرفي.

3- اختلال التوازن النمطي الموحد للتشريعات والقوانين العربية المرتبطة بتكنولوجيات الاعلام والاتصال والوقاية منها.

4- عدم وجود استراتيجية عربية (موحدة او شبه موحدة) مناسبة لصناعة تقنية المعلومات وانعكاس ذلك في انخفاض جهود البحث والتطوير والابتكار لهذه الصناعة .

وبناءً على الاستنتاجات التي توصل اليها البحث يمكن صياغة التوصيات الآتية :

1- اعطاء الاهمية القصوى لموضوع اعادة هيكلة التعليم وبكافة مراحله وتقوية البحث العلمي والتطوير والحث على الابتكار من خلال خطط وطنية مدعومة باتفاقيات اقليمية ودولية.

2- مواكبة التغييرات التكنولوجية المتسارعة لاستيعاب التطورات المستمرة في تكنولوجيا المعلومات والاتصالات وبقية المعارف الانسانية، ومحاولة ممارستها ميدانياً.

3- العمل على ايجاد بيئة مناسبة لبناء صناعة عربية المحتوى متناسقة ومكملة للصناعات العالمية ومطورة لها .

4- العمل على القضاء على الفجوة الرقمية من خلال العمل على انتشار الانترنت وتوسيع استعمالها بما يحقق معرفة تكنولوجية واتصالية متطورة.

5- العمل على تعليم السكان للغات الحية لتمكينهم على الاطلاع المستمر لما يستجد من طرق ومكونات التكنولوجيا المعرفية .

6- زيادة الاهتمام بالعلماء والباحثين وجميع الاختصاصات من خلال تحسين مستواهم المعاشي وتمكينهم على التواصل العلمي في بلدانهم والعمل على جذب الادمغة المهاجرة منهم بخلق الاجواء المناسبة لهم .

« La cybercriminalité est la troisième grande menace pour lesgrandes puissances, après les armes chimiques, bactériologiques, et nucléaires»

Colin ROSE

Etat des lieux des TIC face aux enjeux de la cybercriminalité – le cas de l'Algérie

State of play of ICTs facing the challenges of cybercrime - the case of Algeria

Présentées par :

Dr TALEB Dalila
Maitre de conférences « A»
Faculté d'Economie – TLEMCEN

Dr HALIMI Wahiba
Maitre de conférences « A»
Faculté d'Economie –TLEMCEN-

Resumé :

Avec la mondialisation des échanges, qui a placé les entreprises dans une situation de concurrence internationale accrue, le développement exponentiel des TIC et l'hyper connectivité du monde, dans lequel les informations de toutes sortes circulent sans frontière, l'information est devenue une matière première stratégique que les entreprises doivent savoir maîtriser pour en tirer un avantage concurrentiel.

La mise à disposition sur le web de nombreux outils et services s'adressant à la population mondiale, a conduit à la croissance des actes cybercriminels qui s'est notamment accélérée

durant ces trois dernières années, et la situation risque de s'amplifier avec la mise à

disposition de : réseaux sociaux, blogs, forums, MySpace, Facebook, Youtube, Twitters,…etc. La cybercriminalité a pris une part croissante dans le débat public et médiatique sous le double effet de l'accessibilité d'Internet offerte à de nouvelles populations et surtout de la globalisation des échanges. Le phénomène cybercriminel ne se résume donc plus à des actes

isolés, anecdotiques ou spectaculaires, et la cybercriminalité est désormais souvent considérée comme un risque sécuritaire majeur par la plupart des experts.

Mots clés : TIC- réseaux sociaux – cybercriminalité – protection – prévention

Introduction :

L'ère numérique ignore désormais toutes les frontières. Elle permet l'accès à la culture et à la connaissance, favorise les échanges entre les personnes. Elle rend possible la constitution d'une économie en ligne et rapproche le citoyen de son administration. Les technologies numériques sont porteuses d'innovation et de croissance, en même temps qu'elles peuvent aider ou accélérer le développement des pays émergents.

Mais un certain pessimisme vient tempérer cette approche idéaliste. Tous les progrès génèrent aussi de nouvelles fragilités et vulnérabilités propices aux menaces ou aux risques, car ils aiguisent l'imagination des criminels. La cybercriminalité est désormais une réalité. Elle est d'autant plus dangereuse qu'elle pénètre au sein des familles, là où la délinquance ordinaire n'avait pas accès jusqu'à présent.

Beaucoup de pays luttent souvent avec efficacité contre la cybercriminalité tout en renforçant leur sécurité informatique, mais c'est bien loin d'être le cas en Algérie où les pouvoirs publics sont moins soucieux de développer la sécurité web. En fait, l'Algérie est peu connectée, stratégie e-administration et e-santé inexistante et la stratégie « e-Algérie » est encore à ses balbutiements. Plusieurs entreprises algériennes sont à jour déconnectées, les factures, les fiches de paie et bons de commande ne sont pas toujours dématérialisés. Le paiement électronique reste faible, mais cela

n'empêche pas l'Algérie de figurer dans la liste des pays les plus vulnérables en matière de cyber sécurité.

Dans ce cadre, l'Algérie a pris l'initiative de faire une loi qui réglemente et encadre ce genre de délinquance, elle est donc spécifique, relative à la protection, la prévention et à la lutte contre toutes formes d'infractions liées aux TIC.

A la lumière de ce qui précède, nous avons illustré notre problématique, on se posant la question suivante : *Quel est l'Etat des lieux des TIC face à ce phénomène de cybercriminalité en Algérie ?*

- L'importance de cet article est de mettre en évidence l'état des lieux de cybercriminalité en Algérie et de son impact en matière des TIC.

- Prêter une attention suffisante des autorités publiques, des banques et tout étudiant et enseignant sur le sujet et l'implication d'une cybersécurité sur l'échelle nationale;

- Afin de répondre à la problématique posée on suppose l'hypothèse suivante :

Les moyens de lutte contre la cybercriminalité restent insuffisants face à l'incompréhension, l'incompétence et l'absence de formation des autorités concernées.

La méthodologie de ce travail s'articule autour de trois sections comme suit :

SECTION I : Leconceptetl'objetde la cybercriminalité

Le terme *cybercriminalité* demeure difficile à conceptualiser, car il n'est l'objet d'aucune définition légale (**I**). Ce choix des législateurs a conduit la doctrine à multiplier les définitions de ce terme[1], contribuant

[1]El Zein .S « L'Indispensable Amélioration des Procédures Internationales pour Lutter Contre la Criminalité Liée à la Nouvelle Technologie *in* M.-C. PIATTI : Les Libertés

ainsi à rendre plus complexes les analyses juridiques. En effet, l'absence de définition légale de ce terme est source de confusions, tant au niveau du domaine de la réflexion, qu'au niveau de l'analyse ou du vocabulaire choisi. Ces confusions nous ont conduit à élaborer une définition pratique (**II**) de ce qu'est la cybercriminalité, afin d'appréhender son phénomène.

I) – L'absence de définition légale de la cybercriminalité

La cybercriminalité n'étant pas définie avec rigueur, elle conduit vers des dérivesterminologiques. Ainsi, MM. Alterman et Bloch retiennent comme définition du délitinformatique, la définition de la cybercriminalité proposée par des experts del'Organisation pour la Coopération et le Développement Economique (OCDE), à savoir« *tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne untraitement automatique de données et/ou de transmissions de données* »[1]. Ces juristes,intégrant dans leur définition la notion morale, semblent considérer que le droit pénal nepeut à lui seul contenir toute l'approche « sanction » de l'utilisation frauduleuse del'informatique. Cependant, cette démarche ne saurait être retenue dans la mesure où leschartes de règlement des litiges, telle la charte de l'Internet par exemple, ont révéléleurs limites comme monde alternatif de règlement des conflits. L'application de lanorme pénale se pose ainsi comme solution face à l'échec de ces initiatives[2].

La confusion opérée par ces auteurs, entre la cybercriminalité et le délit informatique, s'avère symptomatique d'une difficulté d'appréhender

---

Individuelles A l'Epreuve des Nouvelles Technologies de l'Information »(Lyon, Presse Universitaires de Lyon), 2001, p. 153.

[1]Alterman .H et Bloch .A « La Fraude Informatique (Paris, Gaz. Palais) » ,3 sep. 1988, p. 530.

[2]ibid

cette forme de délinquance. Ceconstat légitime l'approche du Professeur Lucas qui considère que « *la seule démarcheacceptable consiste à réserver l'acception de fraude informatique aux hypothèses danslesquelles la technique informatique est au coeur de l'agissement incriminable* » *tout ensachant fort bien qu'il est parfois difficile d'isoler le* « *noyau dur* » *de la*« *périphérie* »[1].

La nécessaire clarification des actes qui relèvent de la cybercriminalité a conduit ladoctrine à multiplier les notions désignant les actes illégaux en rapport avecl'informatique. Cette démarche a engendré une pléthore de définitions doctrinales de lacybercriminalité en Europe (**1**) et aux Etats-Unis (**2**).

1. *Une pléthore de définitions adoptées en Europe*

Aucun texte législatif ou réglementaire ne définit la cybercriminalité. Toutefois,certaines notions proches, telles que la criminalité informatique, l'infractioninformatique, le délit informatique ou l'usage abusif de l'informatique, ont fait l'objetde définitions posant la question de l'assimilation ou de la distinction du crime et de lacybercriminalité. Selon le ministère de l'Intérieur français, la cybercriminalité recouvre« *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux detélécommunications en général et plus particulièrement sur les réseaux partageant leprotocole TCP-IP*[2]*, appelés communément l'Internet*». Selon l'O.N.U., la« *cybercriminalité* » doit recouvrir « *tout comportement illégal faisant intervenir desopérations électroniques qui visent la sécurité des systèmes informatiques et desdonnées qu'ils traitent* », et dans une

[1]Lucas.A « Le Droit de l'Informatique » (Paris, PUF), 1987, n° 413.

[2]Désigne les protocoles communs de communication utilisés par l'Internet, permettant l'interconnexion généralisée entre réseaux hétérogènes.

acception plus large « *tout fait illégal commis aumoyen d'un système ou d'un réseau informatique ou en relation avec un systèmeinformatique* »[1].

Pour l'Office fédéral de la police suisse, la cybercriminalité s'entend « *desnouvelles formes de criminalité spécifiquement liées aux technologies modernes del'information, et de délits connus qui sont commis à l'aide de l'informatique plutôtqu'avec les moyens conventionnels* ». Enfin, le Collège canadien de police définit lacybercriminalité comme « *la criminalité ayant l'ordinateur*[2]*pour objet ou pourinstrument de perpétration principale* ».

---

[1]Dixième Congrès des Nations Unies, à Vienne, sous le titre « la prévention du crime et le traitement desDélinquants », [10 – 17 avril 2000], disponible sur :

[2]En effet, la langue française distingue deux mots: l' « informatique » et l' « ordinateur ». En 1965, l'Académie française définissait l'informatique comme « le support des connaissances économiques, sociales et scientifiques en particulier pour les machines automatiques. Ces machines sont les ordinateurs, qui traitent l'information dans tous les domaines ». Voir Blanquet .N« La Protection des Programmes d'Ordinateurs » (Mémoire, Paris II), 1979 p. 6 ; Khater .N « La Protection Juridique du Logiciel Dans le Cadre de la Propriété Intellectuelle Dans les Pays de Langue Arabe » (Thèse, Nantes), 1995, p. 2 ; Gilli .G.P : Le Juriste et l'Ordinateur (Paris, Chron.),1967 p. 47. Dans le domaine informatique, comme dans d'autres domaines, on distingue différentes générations, le passage de l'une à l'autre étant marqué par un saut technologique. La nouvelle génération est caractérisée par les Robots, disponible sur <http://www.robots.net>. Ce terme a été utilisé pour la première fois en 1921 par l'auteur Karel Capek (1890 -1938) dans une pièce de théâtre s'appelée (*Rossum'sUniversal Robots*). L'origine du terme vient du mot *Robota*, qui signifie le travail forcé FIEVET : Les Robots (Que sais-je ? Puf) 2001 p.19; Il est à noter aussi que l'intelligence artificielle a donné lieu à deux courants de pensée.
L'hypothèse forte affirme qu'une machine universelle de Turing dotée d'un programme adéquat serait le siège d'un esprit conscient, comme vous et moi L'hypothèse faible prétend, au contraire que cette voie ne peut mener

Cependant, ces définitions ne sont pas complètement définitives : la définitionadoptée par le ministère de l'Intérieur français vise seulement les infractions dirigéescontre les réseaux de télécommunications. Elle ne recouvre ni les infractionssusceptibles d'être commises sur les systèmes informatiques, ni les infractionsdirectement générées par le fonctionnement des réseaux informatiques. Il s'agit desinfractions portant sur l'information véhiculée par le système informatique commel'escroquerie, l'abus de confiance, et les atteintes aux libertés individuelles par lacréation illicite de fichiers nominatifs[1]. De même, la définition proposée par l'O.N.U.utilise le terme *comportement illégal* pour se référer à la cybercriminalité. Cependant, uncomportement peut être considéré illégal dans un Etat et légal dans l'autre. Enfin, lesdeux dernières définitions considérées par l'Office fédéral de la police suisse, et leCollège canadien de police utilisent des termes très larges qui peuvent recouvrir lacybercriminalité, et la criminalité informatique en même temps. Ces confusions nous ont conduit à nous interroger sur quelques définitions adoptées aux Etats-Unis.

2. *Une pléthore de définitions adoptées aux Etats-Unis*

Aux Etats-Unis, la cybercriminalité forme une grande proportion des délits examinés par la police [2].Son concept diffère d'un Etat à l'autre, et

---

dans le meilleur des cas qu'à une simulation réaliste. Voir Heudin J.C« La Vie Artificielle » (Paris, Hermes),1994, pp. 177 et s;Remy .C : L'Intelligence Artificielle (Paris, Dunod), 1994 pp.20 et s; V° aussi : Murphy .B : *The computer in Society* (Kent, Anthony Blond), [sans date] pp.53-61 ; Devergies .C « L'Impact de l'Utilisation des Technologies de l'information et la Communication, dans l'Entreprise, sur la Vie Personnelle du Salarié » (Université Lille II, Mémoire DESS),2004.

[1]Romain .G « La Délinquance Informatique : Où en Est-on ? (Sécurité Informatique) » Juin 1998, n° 20, p. 1.

[2]Chawki.M « Essai sur la Notion sur la cybercriminalité » IEHEI , juillet 2006, p.9

d'un département de police à l'autre. Selon le Département de la justice (*United States Department of Justice*) lacybercriminalité est considérée comme « *une violation du droit pénal impliquant laconnaissance de la technologie de l'information pour sa perpétration, soninvestigation, ou ses procédures pénales* »[1]. De son côté, le Code pénal de Californie(section 502), définit une liste d'actes illicites qui tombent sous le coup de lacybercriminalité. Il considère comme cybercriminalité le fait « *d'accéder, ou depermettre intentionnellement l'accès, à tout système ou réseau informatique afin : a) deconcevoir ou réaliser tout plan ou artifice pour frauder ou extorquer ; b) d'acquérir del'argent, des biens, ou des services, dans le but de frauder ; c) d'altérer, de détruire, oud'endommager tout système, réseau, programme, ou données informatiques* »[2]. Enrevanche, le Code pénal du Texas (section 33.02) va plus loin. Il considère commecybercriminalité, le fait d'accéder à un ordinateur, à un réseau, ou à un systèmeinformatique sans avoir l'autorisation de son maître; La confusion opérée par ceslégislations, entre la cybercriminalité et la criminalité informatique, s'avèresymptomatique d'une difficulté d'appréhender cette forme de délinquance. Ainsi, MALL déclare que « *le terme cybercriminalité ne signifie plus qu'un acte illicite qui estd'une façon ou d'une autre relatif à l'ordinateur* »[3].

II) – La proposition d'une définition

1. *Le domaine de la cybercriminalité*

L'adjonction de préfixe « *cyber* » qui a tendance à apparaître de manière excessive àchaque utilisation d'un concept classique à l'Internet, à

[1]Chawki.M « Essai sur la Notion sur la cybercriminalité », ibid , p.9.

[2]Ibid

[3]Wall .D « *Crime and the Internet* »(N.Y., Routledge), 2001, p. 3.

la « criminalité », permet deretenir deux sortes de relations entre la criminalité et les réseaux detélécommunications. Dans un premier temps, la criminalité peut être en relationdirecte avec un réseau de télécommunication, c'est-à-dire que la loi incriminedirectement un acte qui, si le réseau de télécommunication n'existait pas, l'acte nepourrait pas être réalisé. On pense en l'espèce au piratage des réseaux téléphoniquespour effectuer des appels téléphoniques gratuits[1].

Dans un second temps, la criminalité peut être en relation indirecte avec un réseau de télécommunication, c'est-à-dire que le réseau de télécommunication se comprend comme un outil ou un moyen pour commettre l'infraction[2]. On pense par exemple à l'accès illicite à un système informatique, ou à l'envoi des virus via le réseau Internet.

La cybercriminalité au sens strict du terme s'entend donc de l'ensemble des infractions commises contre ou par un système informatique effectué à travers un réseau de télécommunication.[3]Elle requiert obligatoirement l'intervention directe ou indirecte d'un réseau de télécommunication pour commettre l'infraction[4]. Tous les actes perpétrés contre l'assurance de la confidentialité, de l'intégrité, ou de la disponibilité des données ou des opérations de traitement, sont commis dans un environnement électronique impliquant un réseau de télécommunication sont considérés comme une cybercriminalité. Maintenant la plupart des ordinateurs - et par la nature même de la cybercriminalité - tous les

[1]Bensoussan .A « Les Télécoms et le Droit »(Paris, Hermes), 1996 pp. 447-483.

[2]*Ibid*p 484 et s.

[3] Le Coq .J.F« La Cybercriminalité (Mémoire D.E.A., Montesquieu Bordeaux IV) », 2000, p. 8.

[4]Shinder .D « The Scene of the Cybercrime(SYNGRESS) », 2002, p. 94.

ordinateurs qui sont impliqués dans ce genre d'infractions sont connectés à un réseau de télécommunication lequel peut être un réseau local, global ou les deux ensembles.

2. *La définition proposée*

La cybercriminalité peut être définie comme : toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite[1].

Sous cette définition, nous pouvons identifier les quatre rôles que joue le système informatique dans les actes illicites :

Objet : Des cas concernant la destruction de systèmes informatiques, ainsi que des données ou des programmes qu'ils contenaient, ou encore la destruction d'appareils fournissant l'air climatisé, l'électricité, permettant aux ordinateurs de fonctionner.

Support: Un système informatique peut être le lieu où le support d'uneinfraction, ou un ordinateur peut être la source ou la raison d'être de certainesformes et sortes d'avoirs qui peuvent être manipulés sans autorisation.

[1]La notion d'interconnexion est au cœur du processus d'ouverture à la concurrence des services de communications électroniques. Pour être effective, une telle concurrence doit impérativement passer par un accès à tout réseau ouvert au public. La directive 2002/19/CE du 7 mars 2002 fixe donc deux principes fondamentaux au régime de l'accès et de l'interconnexion, qui font la matière des deux premiers paragraphes de l'article L. 34-8 du CPCE : l'interconnexion ou l'accès d'une part, les exploitants de réseaux ouverts au public d'autre part. L'interconnexion ou l'accès font l'objet d'une convention de droit privé entre les parties concernées, convention qui est communiquée à l'ART (CPCE et T. art. L. 34-8-1).

Outil : Certains types et certaines méthodes d'infraction sont complexes pournécessiter l'utilisation d'un système informatique comme instrument. Unsystème informatique peut être utilisé de manière active comme dans lebalayage automatique de codes téléphonique afin de déterminer les bonnescombinaisons qui peuvent être utilisées plus tard pour se servir du systèmetéléphonique sans autorisation.

Symbole : Un système informatique peut être utilisé comme symbole pourmenacer ou tromper. Comme, par exemple, une publicité mensongère deservices non existants, comme cela a été fait par plusieurs clubs de rencontresinformatisés.

Le phénomène de cybercriminalité a été amplifié avec les TIC, surtout avec Internet. Il est devenu source de profits, générant plusieurs milliards de dollars, son attractivité est tellement grande que des milliers d'internautes, en quête d'argent facile, s'y laissent tenter. Certains cybercriminels se contentent de fabriquer des logiciels malveillants, d'autres les utilisent afinde perpétrer des actions criminelles[1], des « mafias » structurées, des « script-kiddies »[2], etc

SECTION 2: Le concept des TIC et l'objet de la cybercriminalité

Les nouvelles technologies d'information et de télécommunication (TIC) sont passées par trois (03) phases d'évolution ; la première était celle de « l'informatique centralisée », vers le milieu des années 60 jusqu'à la fin des années 70, où des systèmes d'orientation assistés par rdinateur ont été élaborés pour montrer le potentiel de ces technologies Puis, vient la

[1]Matignon .E, « la cybercriminalité : un focus dans le monde des télécoms », Mémoire de magistère, Université Paris 1 Panthéon-Sorbonne, 2012, p 8.

[2]Un groupe de jeunes adolescents âgés de 12 à 13 ans forment un réseau organisé qui a pour action des usages déviants et frauduleux.

seconde phase qui a été celle des « micro-ordinateurs », au début des années 80 jusqu'au milieu des années 90, où son avènement a rendu l'utilisation interactive plus économique et a facilité la création et la diffusion de programmes simplifiés. Enfin, la troisième phase a été celle de l'utilisation « d'Internet » dès la fin des années 90.

I) Les Technologies de l'Information et de la Communication (TIC) : Unetroisième révolution

Depuis leurs émergences, dès les années 1990, les technologies de l'information et de la communication (TIC) n'ont guère arrêté de poursuivre leur essor dans les pays de toutes les régions du monde, permettant à un nombre croissant de personnes d'être connectées. En effet,

de plus en plus de pays atteignent une masse critique en termes d'accès et d'utilisation des TIC, ce qui accélère la diffusion de ces technologies et stimule encore davantage la demande générée par le développement de l'internet et des abonnements au cellulaire. Avant de mettre le cap sur l'évolution des TIC et de démontrer la fracture numérique persistante entre régions du monde, nous allons d'abord définir la terminologie de ce terme.

Pour les banques, investir dans les TIC correspond « à l'acquisition de matériel et de logiciels destinés à être utilisés dans la production pendant plus d'un an. Les TIC se composent de trois éléments : matériel informatique (ordinateurs et accessoires), équipement de communication et logiciel. L'élément logiciel se compose de logiciels standards, de logiciels sur mesure et de logiciels développés en interne. Cet indicateur s'exprime

en pourcentage de formation brutede capital fixe non résidentielle »[1]. Avant internet, d'autres moyens l'ont précédé impliquantle client en tant que coproducteur de la prestation bancaire[2]. Mais, ce rôle n'a cessé depuis des'accroître et connaît de nouveaux développements.

Aujourd'hui, des organismes tels l'ONU, la Banque mondiale ou l'ITU[3]11 considèrent que les TIC sont des facteurs et non des conséquences du développement économique. Elles disposent de trois caractéristiques :

Omniprésence :c'est-à-dire que ces technologies sont présentes dans la plupart dessecteurs comme l'éducation, la santé, la finance… ;

Amélioration :elles ne cessent de progresser et d'évoluer, en contribuant ainsi à labaisse des coûts pour les utilisateurs, autre à faciliter le quotidiens des usagers ;

Source d'innovation :en plus de leur évolution propre, ces technologies contribuent àl'élaboration de nouveaux produits ou processus.

1. Les TIC, une troisième révolution ?

De par ces caractéristiques, les TIC contribuent au développement d'autres pans entiers del'économie. On pourra ainsi dire qu'il s'agit d'une révolution informationnelle. D'abord, carelle a été jaugée par la plupart comme étant « la troisième révolution », classée parmi lesmouvements les plus dominants qui ont participé au bouleversement de l'histoire économique

---

[1]OCDE (2020), « Investissement dans les TIC (indicateur) ». doi: 10.1787/dce9bb90-fr (Consulté le 21 mars 2020) http://data.oecd.org/fr/ict/investissement-dans-les-tic.htm

[2]Rowe, « impact de l'information sur la performance de l'entreprise »,1994, p. 256

[3]IUT : International Union of Télécommunication, (en Français l'UIT : l'Union Internationale desTélécommunications), est un organisme de division de données et de statistiques sur les TIC dans le mondeentier, Genève en suisse.

Après la révolution industrielle et l'invention de l'électricité, l'ère des TIC arrive enprovoquant des modifications profondes dans la structure de l'économie mondiale. Ainsi,durant sa diffusion, les grandes nations ont vécu une croissance forte et dure, permettant lepassage de ces dernières d'une économie traditionnelle appuyée sur les ressources commerichesse des nations à une nouvelle économie[1]fondée sur le savoir qui porte surl'information et la communication.

« Dans les nouvelles économies, la technologie est le conducteur majeur non juste de laqualité de vie améliorée pour le peuple sous développé ou en voie de développement maisaussi un levier du développement économique pour les pays industrialisés, développés etmême les pays émergents.»[2]

2. Etat des lieux des TIC

A l'heure actuelle, plus de la moitié de la population mondiale est connectée. Fin 2018, 51,2 pour cent de la population, soit 3,9 milliards de personnes, utilisaient l'Internet, ce qui représente une avancée importante dans le sens d'une société mondiale de l'information plus inclusive. Les pays développés, dans lesquels quatre personnes sur cinq sont connectées, sont proches de la saturation. Dans les pays en développement par contre, il reste encore beaucoup à faire pour améliorer la croissance, puisqu'on ne compte que 45 pour cent d'internautes. Dans les 47 pays les moins avancés (PMA), l'adoption de l'Internet reste relativement limitée, quatre personnes sur cinq (80 pour cent) n'utilisant pas encore l'Internet.

---

[1]**Nouvelle économie** désigne la croissance générée à partir de la fin des années 1990

[2]Ben Youssef .A, M'Henni .H, « Les effets des technologies de l'information et de communication sur la croissance économique : cas de Tunisie », Région et Développement n°19, 2004, pp 132-135

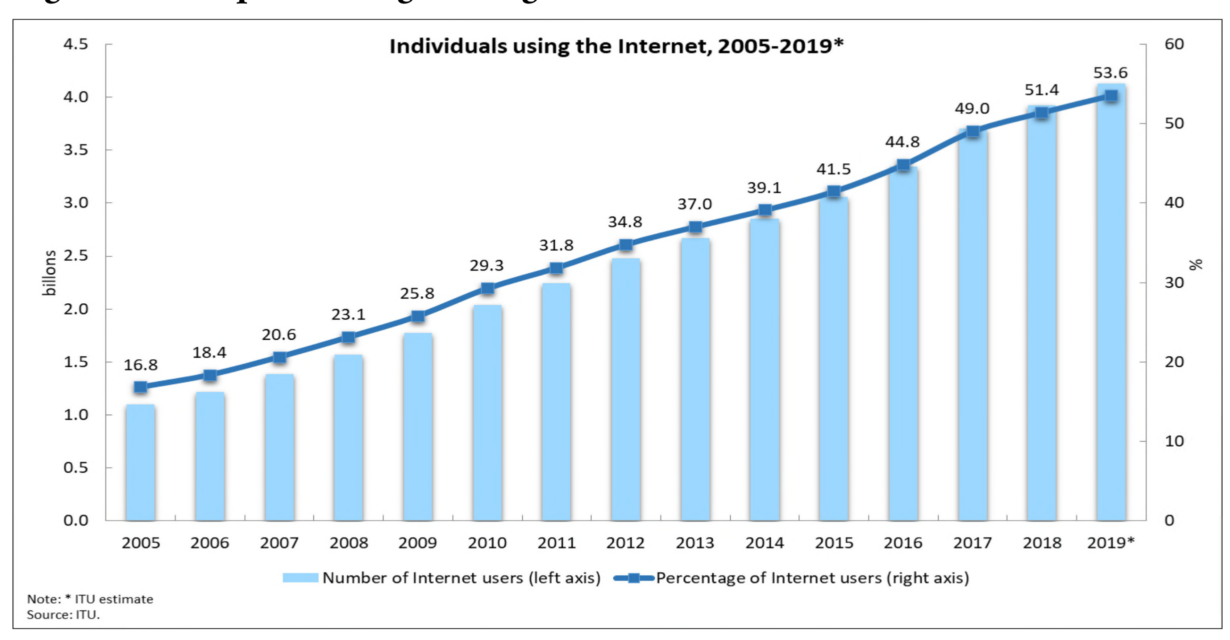
On continue d'observer une tendance générale à la hausse en ce qui concerne l'accès aux TIC et l'utilisation de ces technologies. Exception faite de la téléphonie fixe, tous les indicateurs font apparaître une croissance soutenue au cours des dix dernières années. Cependant, la croissance a connu dernièrement un fléchissement pour la plupart des indicateurs relatifs à l'accès, en particulier dans les pays où une grande partie de la population est déjà connectée. La croissance devra recommencer à augmenter si l'on veut atteindre les objectifs ambitieux du Programme Connect 2030 de l'UIT et de la Commission "Le large bande au service du développement durable", qui prévoient un taux de pénétration de l'Internet de 70 pour cent d'ici à 2023 et de 75 pour cent d'ici à 2025.

L'accès mobile aux services de télécommunication de base est de plus en plus répandu ;Alors que le nombre d'abonnements à la téléphonie fixe poursuit sa baisse à long terme, le nombre d'abonnements à la téléphonie cellulaire mobile continue de croître et a d'ores et déjà dépassé la population mondiale, encore que cela ne soit pas le cas dans toutes les régions. En conséquence, il est à prévoir que les pays en développement, et tout particulièrement les PMA, rattraperont peu à peu leur retard par rapport au reste du monde.**L'accès au large bande continue d'enregistrer une croissance soutenue.** Le nombre d'abonnements au large bande fixe ne cesse d'augmenter, sans que cela entraîne un ralentissement des taux de croissance. De surcroît, pour la quasi-totalité des abonnements au large bande fixe, les débits de téléchargement se sont établis à au moins 2 Mbit/s et, pour une très grande partie d'entre eux, à plus de 10 Mbit/s. Dans les PMA, le nombre d'abonnements pour la catégorie de débit la plus faible (≥256 kbit/s à <2 Mbit/s) demeure important, encore que cette proportion diminue rapidement. S'agissant des abonnements actifs au large bande

mobile, la croissance a été nettement plus forte, puisque les taux de pénétration sont passés de 4,0 abonnements pour 100 habitants en 2007 à 69,3 abonnements pour 100 habitants en 2018.

La quasi-totalité de la population mondiale vit aujourd'hui dans une zone desservie par un signal mobile cellulaire,De plus, la plupart des utilisateurs peuvent avoir accès à l'Internet intermédiaire d'un réseau 3G ou d'un réseau de meilleure qualité ;Il convient cependant de noter que cette évolution des réseaux mobiles est plus rapide que l'accroissement du pourcentage d'internautes. Comme nous verrons ci-dessous

Figure 01 : le pourcentage d'usagers d'internet durant 2005-2019



Selon le rapport de l'UIT, la cybercriminalité est souvent présentée par une dimensioninternationale. Les contenus illicites qui se transmettent par courrier transitent souvent parplusieurs pays avant d'atteindre leur destinataire. Ils sont parfois stockés à l'étranger, c'estpourquoi les Etats concernés par un cyberdélit doivent collaborer aux enquêtes diligentées[1],

[1]Putnam/Elliott, « International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism », 2001, p.35.

partout dans le monde, l'informatique repose fondamentalement sur la même technologie.

Lesordinateurs et les téléphones portables vendus en Asie ressemblent de très près à ceux vendusen Europe. Même chose pour le cas d'Internet, car avec la normalisation des réseaux, les paysafricains utilisent les mêmes protocoles que les Etats Unis[1]. C'est pour cela que lesinternautes du monde entier peuvent avoir accès aux mêmes services. L'harmonisation desnormes techniques a donc permis la mondialisation des technologies et des services, seulement elle devrait également conduire à l'harmonisation des législations nationales (ce qui pourrait être une bonne initiative pour l'Algérie). Comme l'ont démontré les négociations de la convention du Conseil de l'Europe sur la cybercriminalité, le droit national évolue beaucoup plus lentement que les techniques.

3. Les motivations des cybercriminels

Le cybercrime est une activité à croissance démesurée. Les opérations de cybercrime ont comme facteur commun l'anonymat virtuel dont profitent les cyber-attaquants, car leurs chances d'être détectés sont moindres. Cette activité attire différents types de personnes qui utilisent leurs propres techniques et méthodes pour s'impliquer, ils ont des motivations propres à eux. Il est parfois difficile de cerner toutes les motivations des cybercriminels mais en gros, on peut distinguer quatre (04) des plus majeures[2]:

[1]Les plus importants protocols d'informations sont : TCP (transmission control protocol) et le IP (Internet Protocol) ; pour plus d'information voir: Tanebaum, « Computer Networks », 2002; Comer, « Internet workingwith TCP/IP – Principles, Protocols and Architecture », 2006.

[2]Souligné par les synthèses « SOLUCOM », Management & IT consulting, Observatoire de la transformation

3-1) L'idéologie : elle vise à défendre une conviction (politique ou religieuse). A travers des attaques, le cybercriminel a pour objectif d'interrompre des services, à diffuser des messages partisans ou à divulguer les données d'une entreprise et ainsi nuire à son image ;

3-2) Les gains financiers directs : pour la majorité des cybercriminels, l'argent est la principale motivation[1], il s'agit, par exemple, du vol de données bancaires (en particulier des numéros de cartes), de données personnelles mais aussi de données critiques de l'entreprise comme les secrets industriels ou les informations concernant sa stratégie. Elles seront revendues par la suite ou utilisées pour réaliser des fraudes ;

3-3) La déstabilisation entre Etats ou le Cyberterrorisme : est une motivation à laquelle visent les cybercriminels par la destruction des systèmes ou le vol de données stratégiques qui pourraient nuire au bon fonctionnement des services vitaux des Etats ;

3-4) L'obtention de capacités d'attaques : autre motivation qui se développe. Elle consiste àvoler les secrets des mécanismes de sécurité (mots de passe, certificats, failles de sécurité, etc.) ou à attaquer les SI (Système d'Information) des fournisseurs (info-gérants, opérateurs de télécom, fournisseurs de solution de sécurité) de sociétés qui seront visées ultérieurement.

Ces éléments sont utilisés plus tard pour lancer la véritable attaque. Les cybercriminels ne se fixent plus aucune limite dans la réalisation de leurs desseins. De nos jours, ces attaques peuvent toucher n'importe quelle

---

des entreprises, n° 47, sur la Cybercriminalité : comment agir dès aujourd'hui, Octobre 2013

[1]D'après les données du Kaspersky Lab, < http://blog.kaspersky.fr/quest-ce-qui-motive-les-cybercriminelslargent-evidemment/372/ >

entreprise, quel que soit son secteur d'activité. Comme l'a récemment montré l'actualité, ce schéma ci-dessous résume les quelques organismes et Etats qui ont été victimes de cyber attaques :

Figure 02 : Les motivations des cybercriminels et quelques exemples d'Etats ou

entreprise ciblés



Source : Les synthèses « SOLUCOM », Management & IT consulting, Observatoire de la transformation des

Entreprises, n°47 sur la cybercriminalité : comment agir dès aujourd'hui, Octobre 2013, p 4

- **L'expérience française face à la cybercriminalité**

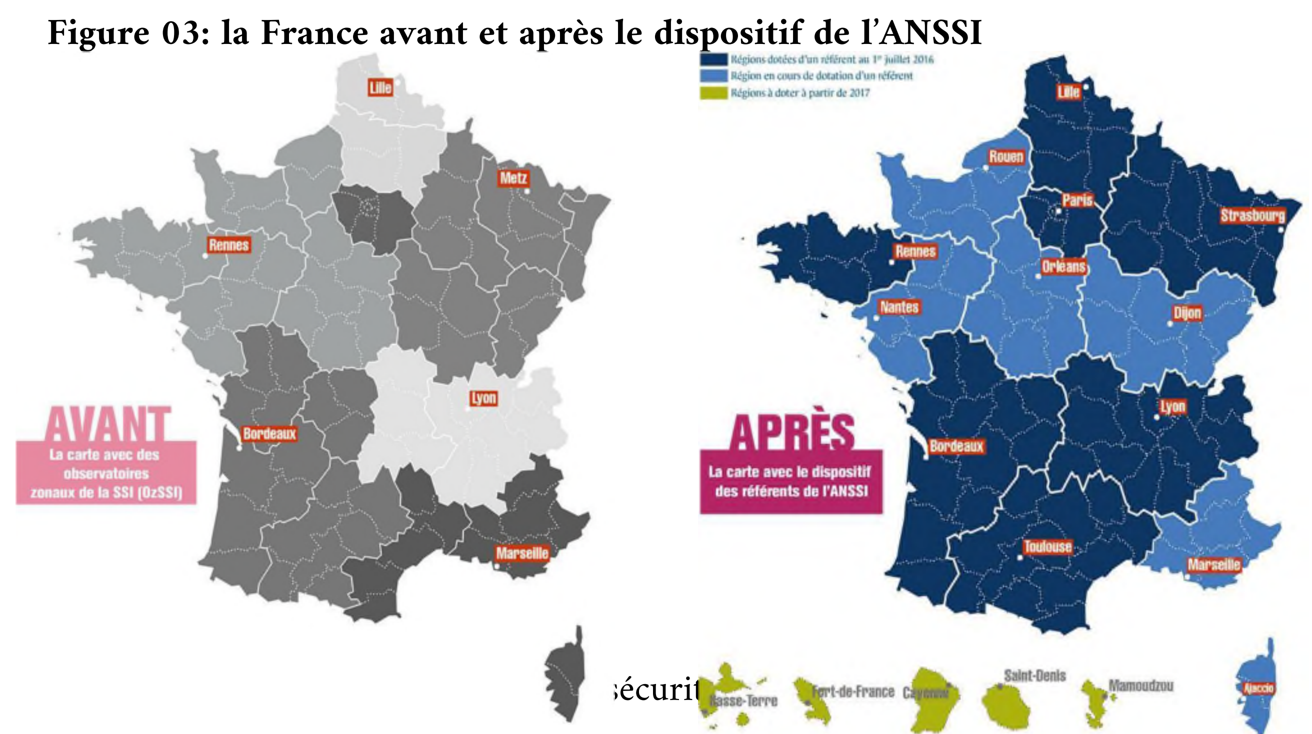
L'actualité de la question d'une « cyber défense » et d'une « cyber sécurité », dévoile la nécessité de chaque Etat de disposer d'une stratégie globale et d'une grille juridique cohérente. Les spécialistes rencontrent de réelles difficultés à cerner le phénomène et appréhender le contenu technique et apporter des réponses pertinentes, En Europe, la lutte contre la cybercriminalité repose sur une coopération internationale qui rassemble

entre le prolongement de l'activité opérationnelle des services d'enquête et des autorités judiciaires.

Pour faire face aux risques d'attaques informatiques, l'ANSSI[1] (Agence Nationale de Sécurité des Systèmes d'Information), créée en juillet 2009, se voyant confier des missions dedéfense des systèmes d'information, aboutit, en 2010, à la définition d'une stratégie nationalede défense et de sécurité des systèmes d'information par la France,L'article 22 de la loi sur la réglementation militaire édictée en 2013 a euen effet, pour conséquence de faire monter le niveau de sécurité des opérateurs. Les grandes entreprises doivent désormais mettre en place des systèmes de détection et rendre compte à l'agence de toutes les attaques dont elles ont fait l'objet

[1] l'ANSSI a un rôle qui est d'ordre préventif: elle joue, le rôle d'expert étatique s'agissant de la sécurisation des
systèmes d'information auprès des administrations comme des opérateurs sensibles. Elle réalise donc, des diagnostics (sur les moyens de communication sécurisés de l'Etat ou, pour prendre des exemples intéressants le système judiciaire, les bracelets de surveillance électronique, la gestion des clés dans les établissements pénitentiaires, la future plate-forme des interceptions judiciaires...), fait des recommandations (par exemple, sur les badges d'accès, la vidéo-surveillance...). Elle assure, aussi, une mission d'audit et d'inspection, à la fois au plan organisationnel et s'agissant des risques d'intrusion (centrales nucléaires, tunnel sous la Manche, application pénale Cassiopée...). Elle exerce, encore, un contrôle sur les investissements étrangers dans le domaine de la sécurité informatique. Elle entretient, enfin, des relations étroites avec les organismes comparables
des pays étrangers.

Figure 03: la France avant et après le dispositif de l'ANSSI



sécurit
des territoires » rapport de la CEIS, janvier 2020, p20.

Depuis décembre 2015, L'ANSSI s'est décentralisée pour renforcer la cybersécurité des territoires avec le déploiement de référents en régions. Ce déploiement est le fruit d'une réflexion interministérielle, sur l'avenir de l'action territoriale en matière de sécurité numérique. Il indique la nécessité d'un lien renforcé et permanent entre l'ANSSI et les régions. Par cette démarche, l'ANSSI, qui travaille sous l'autorité du Premier ministre, souhaite « apporter son expertise de la prévention des incidents et remplir au mieux sa mission de sensibilisation aux bonnes pratiques informatiques Les agents mobilisés sont des experts de la sécurité informatique chargés d'aller à la rencontre des préfets, des collectivités locales, des responsables de chambre de commerce, en organisant notamment des séminaires de sensibilisation aux risques et menaces cyber, en coordination avec les préfectures. En cas d'incident, ces référents peuvent faire office de filtres : selon le niveau de gravité d'une attaque, ils peuvent décider de transmettre

à l'ANSSI directement ou bien aux forces de police, également compétentes dans le règlement de ce type d'affaires. L'initiative de l'ANSSI témoigne de la réalité des problèmes de cybersécurité dans les entreprises Sont notamment visés les sites industriels sensibles, comme le « couloir de la chimie » près de Lyon, qui concentre de nombreuses usines pétrochimiques.

La plateforme https://cybermalveillance.gouv.fr lancée en octobre 2017 assume un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de lapopulation française, particuliers, entreprises (TPME voire ETI, artisans, commerçants, hors opérateurs critiques type OIV qui relèvent de l'ANSSI) ou collectivités territoriales (hors OIV). En 2018, l'ANSSI a indiqué avoir observé 391 incidents hors opérateurs d'importance vitale, 16 incidents majeurs et mené 14 opérations de cyberdéfense.

Les obligations réglementaires et normatives s'imposent non seulement aux opérateurs d'importance vitale (OIV) mais aussi à l'ensemble des entreprises dépositaires de données via le règlement général sur la protection des données (RGPD). Entré en vigueur en mai 2018, ce règlement européen impose une mise en conformité des systèmes d'information et oblige les entreprises dépositaires de données à investir dans des outils et processus de sécurisation de ces dernières. On passe en effet d'une logique de contrôle a priori basé sur des formalités administratives à une logique de responsabilisation des acteurs privés et publics. Ce changement de posture se traduit par une mise en conformité permanente et dynamique de la part des collectivités. Elles devront ainsi :

• Adopter des mesures techniques et organisationnelles pour garantir une protection tout au long du cycle de vie des données

• Démontrer à tout instant qu'elles offrent un niveau optimal de protection aux données traitées.

• Intégrer les principes de protection des données dès la conception (Privacy by design) et par défaut (Privacy by default)

On peut également rappeler l'existence de normes internationales, comme l'ISO 27001, très prisée des donneurs d'ordres publics dans leurs appels d'offres et des offreurs à la recherche d'un avantage concurrentiel.

Sur le plan réglementaire, un référentiel général de sécurité applicable aux collectivités territoriales comme à l'ensemble des autorités administratives a fixé en mai 2010 un cadre visant à instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Ce document a été complété et remplacé par un nouveau référentiel en juin 2014. Dans le prolongement de cette approche, un guide comprenant 42 règles d'hygiène informatique a été publié en janvier 2017. Des outils innovants peuvent par ailleurs favoriser la montée en puissance effective de la cyberdéfense dans les collectivités territoriales, dont seules les plus importantes sont en mesure de se doter en interne des compétences nécessaires pour faire face aux attaques.[1]

SECTION3:la cybercriminalité en Algérie

L'Algérie fait partie des pays qui s'intéressent le moins aux technologies d'information et decommunication, mais ces dernières années le pays essaie de rattraper son retard en multipliantles réformes et les initiatives d'investissement dans le secteur des TIC. L'implication de dernier dans la compétitivité et la croissance et le développement économique est très limitée,malgré l'usage lent mais plus généralisé d'Internet et des moyens

---

[1]Alexandre Mot « La cybersécurité : un nouvel atout au service des territoires » rapport de la CEIS janvier 2020, p 21.

de télécommunication celan'a pas empêché le développement des délits liés à leurs usages.

Selon le rapport de l'Union Internationale de Télécommunication (UIT), sur la sociétéd'information et la pénétration du haut débit dans le monde, l'Algérie ne brille pas par sondéveloppement, en 2014 elle squatte toujours la même place qu'en 2012 et 2013 c'est-à-dire la14ème place, il compté parmi les 5 pays du monde arabe à avoir un indice de développementtrès faible aux coté du Soudan, la Mauritanie, le Yémen et Djibouti. Egalement, d'après lerapport de The Global Information Technology, établie par le World Economic Forum(WEF) [1], l'Algérie gagne 9 places par rapport à l'an passé et prend la 120ème, suivant unclassement sur leur capacité à utiliser les TIC pour améliorer leur compétitivité, leurcroissance et la prospérité des citoyens. Ce rebond en 2015 est dû au fait que le secteuralgérien des technologies de l'information et de la communication s'était d'abord engagé, aucours de ses réformes précédentes avec le soutien de la Banque mondiale, dans une réformedu secteur des postes et des télécommunications (en l'an 2000). Parmi les principalesréussites[2], on site:

-l'adoption d'une déclaration de politique des télécommunications pro-libérale en 2000 ;

- la promulgation de la nouvelle Loi sur les Postes et Télécommunications (Loi 2000-03) du mois d'août 2000 ;

---

[1]Le rapport, « The Global Information Technology », SoumitraDutta (CornellUniversity), Thierry Geiger, (World Economic Forum), Bruno Lanvin (INSEAD), 2015, p 119, accessible sous format PDF : http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf

[2]The World Bank, « Fondations for the development of information and communication technologies in Algeria », report No. 25841, Avril 2003, p 15.

- l'établissement d'une entité réglementaire indépendante (ARPT)[1] opérationnelle depuis mai 2001 ;

- la transformation d'Algérie Telecom et d'Algérie Poste en entreprises commerciales, l'octroi

àOrascom Telecom Algérie (OTA) en juillet 2001 de la seconde licence GSM pour 737 millions de dollars US[2].

Par ailleurs, Toutefois, cette amélioration ne reflète pas le classement mondial de l'Algérie dans la vitesse du débit de la connexion qui a reculé à la 182 eme place sur 207 pays en 2019. Avec ce classement l'Algérie perd sept places par rapport à l'année 2018, ou elle était à la 175 éme place.

Toutefois, cette amélioration ne reflète pas le classement mondial de l'Algérie dans la vitesse du débit de la connexion qui a reculé à la 182 eme place sur 207 pays en 2019. Avec ce classement l'Algérie perd sept places par rapport à l'année 2018, ou elle était à la 175 eme place[3].

Selon les statistiques de l'Union Internationale de télécommunication et du site Internet world

statistique[4], en 2019, l'Algérie était au nombre de 25,428.159 d'usagers à Internet ce qui représentait un taux de pénétration de 58.0% dans le pays, qui est faible si on le compare à ses voisins maghrébins tel le Maroc où le taux est de 64,3% ou en Tunisie qui est de 66,8%.

Tableau n° 01 :Nombres d'internautes et taux de pénétration d'Internet

---

[1]ARPT : Autorité de Régulation de la poste et des Télécommunications

[2]BouchelitRym, « Les perspectives d'E-banking dans la stratégie E- Algérie 2013 »,Thèse de doctorat , Tlemcen , 2014-2015,p121.

[3]Pour plus d'information consultez le lien :consulté le 25/03/2020.

[4]Consultez le site : consulté le 30/03/2020

Année	N d'usagers	Population	% Pénétration
2000	50,000	31,795,500	0.2 %
2005	1,920,000	33,033,546	5.8 %
2007	2,460,000	33,506,567	7.3 %
2008	3,500,000	33,769,669	10.4 %
2009	4,100,000	34,178,188	12.0 %
2010	4,700,000	34,586,184	13.6 %
2012	5,230,000	37,367,226	14.0 %
2013	6,404,264	38,813,722	16.5 %
2014	6,669,927	38,813,722	17.2 %
2015	11,000,000	39,542,166	27.8 %
2016	15,000,000	40,263,711	37.3 %
2017	18,580,000	41,063,753	45.2 %
2019	25,428,159	43,851,044	58.0 %

Source : http://www.internetworldstats.com

Malgré les efforts consentit par l'Etat Algérien, le développement du réseau Internet reste limité, avec un taux de pénétration relativement faible de 17,2% comparativement à certains pays du Maghreb. L'Algérie reste un pays consommateur passif des technologies d'Internet elle ne se limite qu'à certaines fonctions basiques à l'instar de la correspondance électronique (mailing) et de la communication (chat, téléphone via Internet), la recherche d'information viales moteurs de recherche et le téléchargement

des softwares, etc. L'Algérie est pratiquement absente du réseau mondial du Web, avec seulement 1400 sites dont 800 sont actifs, l'Algérie est en retard par rapport a certains pays comme le Maroc avec 6000 sites, 4000 pour la Tunisie, et 800000 pour la France. Selon les statistiques du CERIST, le nombre de nom de domaines « .dz » en Algérie est de 2380[1].

II- Cybercriminalité en Algérie

La cybercriminalité ne cesse d'augmenter du fait du développement des Technologies de l'Information et de la Communication (TIC), le développement des nouvelles technologies a ouvert une brèche aux comportements illicites, la cybercriminalité en plein boom, l'escroquerie et l'arnaque deviennent massives, Certes, nos services électroniques ne sont pas assez développés ou quasiment inexistants (comme le e-commerce, le e-santé ou le e-administration). Néanmoins, cela ne doit pas empêcher l'Algérie de se doter d'outils pour se prémunir une fois la technologie introduite car ça reste un phénomène inévitable.

1. Les cyber-attaques contre l'Algérie

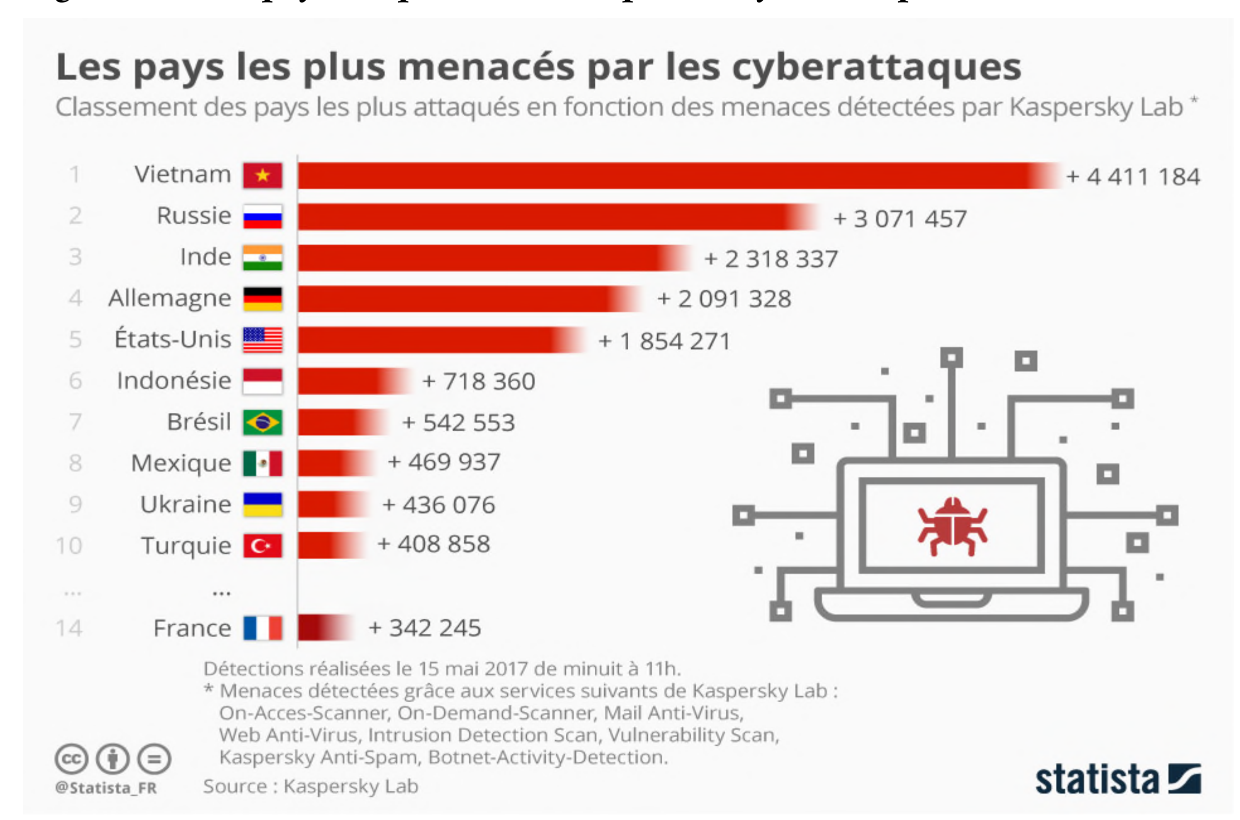
Des institutions algériennes ont été victimes de plusieurs cyber-attaques dont les responsablessont des hackers aux motivations politiques. D'autres attaques plus sophistiquées, ayant pourbut l'espionnage, et qui émane de nations qui ont ciblé notre pays (comme les Etats-Unis).

Des compagnies comme *Microsoft, Kaspersky, The Norman Malware Cleaner, Trendmicro,Seculert, Lookout*et le rapport de septembre 2014 de *l'Europol,* confirment l'appréhensionquant à l'état du cyber espace en Algérie. Du troisième trimestre 2013 au deuxième trimestre2014,

[1]BouchelitRym, op-cit, p 135.

l'Algérie est passé de la 8ème place à la 3ème place des pays les plus infectés dans lemonde. Avec un pourcentage de 52,05%.[1]

Figure 04 : les pays les plus menacés par les cyberattaques en 2017



Source : www.fr.statistica.com

Selon le rapport de la DGSN (direction générale de la sureté nationale)En matière de prévention et de lutte contre la cybercriminalité, le bilan fait ressortir une évolution significative du nombre de dossiers judiciaires formalisés allant de 246 dossiers en 2014, à 567 en 2015 et 1.055 dossiers en 2016, pour atteindre 2.130 affaires en 2017, soit une augmentation de 102% par rapport à l'année 2016, précise la même source. Parmi ces attaques on recense 35,60% des affaires portent sur les atteintes

[1]Les informations bien en détail citées dans le lien suivant : http://www.ssri.dz/la-cyber-securite-etat-des-lieuxen-algerie/

aux biens, 11,04 sur les infractions à la législation des stupéfiants, 4,82% relèvent d'affaires économiques et financières, 11,22% sur les atteintes à la chose publiques, 2,05% sur les atteintes aux bonnes mœurs, 0,93% liées à la cybercriminalités et 34,34% sont des atteintes aux personnes[1].

2. Les Institution chargées de la réglementation

Des institutions sont chargé de la réglementation numérique et du système d'informations,leur objectifs se définis dans la prospérité du secteur des Tic mais également à maintenir uncontrôle et une surveillance en son sein. Parmi elles on site :

Tableau n°2: Entités Algériennes de réglementation

institution	Présentation et mission
ARPT	L'Autorité de régulation de la poste et des Télécommunications, Accès aux réseaux large bande et Radiodiffusion. Veille à la protection du consommateur à la sécurité informatique et à la certification électronique, analyse les différents outils et logiciels de sécurité (en cryptographie), tire le meilleur partie de son système d'information dont les systèmes de pilotage et de production
MPCIT	Ministère chargé de la poste et des technologies de l'information et de la communication ; Autorité gouvernementale qui est responsable des initiatives politiques liées au secteur desTIC en Algérie,il est chargé du

[1]Disponible sur le site : www.aps.dz

suivi et du contrôle de l'activité de liés aux TIC et à laposte ; Autorité de cybersécurité. Depuis peu, elle contrôle la signature et la certification

électronique (loi 15-04 du 1 février 2015).

CERIST	Régulateur national responsable des contenus numériques et centre de recherche surl'information scientifique et technique. Le centre a pu s'ouvrir et développer des solutions à certains problèmes relatifs à la société de l'information et par la même favoriser sapromotion.
TDA	Régulateur national de la Radiodiffusion numérique, chargé de la gestion de l'émission etde la diffusion par voie de terre et par satellite les programmes de radio et Télévision.
CTRF	Cellule de traitement du renseignement financier est un organe spécialisé, indépendant,chargé de recueillir, de traiter, d'analyser et d'échanger avec les organismes homologuesétrangers des renseignements financiers dans le but de contribuer à la détection, préventionet la dissuasion du recyclage de fonds et de financement des activités terroristes en Algérie.

Elle mobilise quatre services : Le service Enquêtes et Analyses ; le service documentation etbases de données ; le service de la coopération ; le service juridique.

III- La mise à niveau du cadre juridique national : *cause ou conséquence*

Avec les nouvelles formes de criminalité qui sont apparues et ont évolué dans le cyber espace,l'Algérie se devait de se doter d'un arsenal juridique et d'adopter des lois spécifiques relativesà la prévention et à la lutte contre les infractions liées aux TIC, il y'eu d'abord la loi n° 04-15du 10 novembre 2004 qui venu apporté les premiers articles de lutte contre ces nouvellesinfractions puis la loi n° 06-23 du 20 décembre 2006 venu compléter celle de 2004 en modifiantet complétant le code pénal. En plus de la loi de 2009 et celle de 2014. Un tableau résume partype d'infraction et les incriminations dans le code pénal algérien voir dans l'annexe n°2.

La lutte contre le phénomène de la cybercriminalité doit inévitablement déboucher sur la miseen place d'institutions étatiques. En effet, il appartient à l'Etat de droit de garantir la sécuritédans le cyberespace et d'établir la confiance numérique, seuls éléments capables de favoriserle développement des nouvelles économies basées sur la dématérialisation des relations et deséchanges[1].

En plus du cadre juridique, duquel elle s'est dotée, l'Algérie doit contourner lephénomène de cybercriminalité et se lancer dans la confiance numérique et la protection desdonnées personnelles[2] : à l'instar des autres pays du Maghreb, l'Algérie dispose d'unepolitique publique pour la confiance numérique. Cette politique est basée principalement surla mise

[1]El Azzouzi .A, « la cybercriminalité au Maroc », édition Ali el AZZOUZI, Casablanca, 2010, p103.

[2]Jankari.R, « Les technologies de l'information au Maroc, en Algérie et en Tunisie », vers une filièreeuromaghrébine des TIC ? », Consultant à l'Institut de Prospérité Economique du Monde Méditerranéen, Etudes
& Analyse, vers une filière euromaghrébine des TIC, Octobre 2014, p 19, 20.

en place d'un dispositif juridique de protection contre la cybercriminalité et lesinfractions qui touchent les systèmes d'information. En 2004, le pays a adopté une série demesures pour lutter contre la cybercriminalité. Il s'agit de :

• la promulgation de la loi 04-15 du 10 novembre 2004 relative aux atteintes des systèmes detraitement automatise de données (STAD) ;

• l'installation du Centre de lutte et de prévention contre la cybercriminalité de la gendarmerienationale ainsi que la mise en place d'autres laboratoires spécialises et des brigadesspécialisées de la direction de la sûreté nationale. La loi 09-04 du 5 aout 2009 relative à laprévention et à la lutte contre les infractions liées aux TIC est un autre texte fondateur dans ledomaine de la confiance numérique. Elle concerne les infractions portant atteinte au systèmede traitement automatise de données telles que définies par le code pénal ainsi que toute autreinfraction commise ou dont l'exécution est facilitée par un système informatique ou unsystème de communication électronique. Cette loi prévoit d'ailleurs la possibilité d'effectuerdes opérations de surveillance des communications électroniques et la perquisition dessystèmes informatiques dans le cas de la protection de l'ordre public et les besoins d'enquêtesou d'informations judiciaires en cours. Dernièrement la loi n°15-04 du 1er Février 2015relative à la signature et à la certification électronique.

Conclusion :

La technologie de l'information et de communication est un outil de modernisation de l'entreprise de l'administration et de l'état.

Néanmoins il faut prendre en compte des cybermenaces et cyberattaques et il est également important de comprendre que les cyberattaques ne peuvent pas être éliminées mais peuvent être gérées.

Mais malgré les cybermenaces très évidente, l'attitude à l'égard des descyberattaques demeure celle-ci « ça ne m'arrivera pas à moi ».

La réalité de la cyberattaquene consiste pas à se demander « si » cela se produira, mais bien « quand » cela se produira et « par qui ».

Il faut donc déplacer les efforts sur comment les entreprises et les gouvernements peuvent résister et réagir à une cyberattaque réussie.



المحور الثاني

صور الجريمة المعلوماتية

الحماية الجزائية لحقوق الأفراد من الممارسات التعسفية لحرية التعبير
-بين المفهوم التقليدي ومتطلبات مواكبة التطور الإلكتروني-

Criminal protection of individual rights against arbitrary freedom of expression

-Between the traditional concept and the requirements to keep up with electronic development-.

د. محمد هاملي أستاذ محاضر قسم "أ"
معهد الحقوق والعلوم السياسية
المركز الجامعي -مغنية-

مقدمة:

مع تطور التقنية ظهرت إلى ساحة الوجود أنماط جديدة ووسائل عدة للتعبير عن الرأي تجاوزت كل الحدود الجغرافية، بل وفي كثير من الأحيان تجاوزت حتى الحدود الأخلاقية، وهو ما ألقى على عاتق المشرع الجزائي الجزائري مسؤولية كبيرة في التصدي للتجاوزات التي قد تحدث.

وبالفعل، فقد حاول المشرع القيام بالدور المذكور من خلال وضع جملة من الأحكام لغرض ردع السلوكات التي تنطوي على اِعتداء على مصالح الأفراد تحت غطاء حرية التعبير، بعضها أورده في قانون العقوبات، وبعضها أورده في القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، وبعضها الآخر أورده في القانون رقم 18-04 المتعلق بالبريد والمواصلات الإلكترونية[2]، فيما أورد بعض الأحكام في القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[3].

[1]. القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47 الصادر بتاريخ 16 أوت 2009.

[2] . القانون رقم 18-04 المؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، جريدة رسمية عدد 27 الصادر بتاريخ 13 مايو 2018.

[3] . القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34 الصادر بتاريخ 10 يونيو 2018.

والتساؤل الذي تطرحه هذه الدراسة، هل إستطاع المشرع الجزائي الجزائري مواكبة التطورات الحاصلة في المجال المعلوماتي وأرسى من القواعد ما يسمح بالتصدي لجرائم التعبير الماسة بحقوق الأفراد التي أفرزتها هذه التطورات؟ أم أنه لا يزال حبيس المفاهيم التقليدية؟

إن الإجابة على هذا التساؤل تكتسي أهمية بالغة، إذ من شأنها أن تسلط الضوء على مواطن القصور في القانون الجزائري، والتي قد تؤدي إما إلى الإفلات من العقاب لعدم إحاطة الأحكام الجزائية بوسائل الاتصال الإلكترونية، أو على العكس قد تؤدي إلى مغالاة في تطبيق بعض الأحكام بسبب التقدير المبالغ فيه لخطورة بعض الأفعال، وهو ما يؤدي إلى زيادة القيود على حرية التعبير. ولأجل الوصول إلى الغاية المرجوة، ستركز هذه الدراسة على البحث فيما إذا كان المشرع الجزائي الجزائري يشترط عنصر العلانية في كافة الجرائم المتعلقة بالتعبير عن الرأي والماسة بحقوق الأفراد أم أنه يشترطها في بعضها فقط، وما إذا كانت أشكال العلانية في حال إشتراطها تتّسع لتستوعب طرق الاتصال الإلكتروني الحديثة. ولكن قبل ذلك، ينبغي تحديد إطار الدراسة بدقة، فالبحث في الجرائم المتعلقة بحرية التعبير الماسة بحقوق الأفراد يقتضي توضيح مدلول هذه الحرية وتمييزها عن بعض الحريات المشابهة لها.

في هذا الصدد، يميل الرأي الراجح لدى الفقه إلى تعريف حرية التعبير على أنها حق الإنسان في أن يعتنق من الآراء التي يشاء، وحريته في نشرها وإذاعتها بوسائل الإعلام كافة من كتّابة وطباعة وإذاعة وسينما ومسرح[1]. وبذلك فهي تختلف عن حرية الرأي التي تعرّف على أنها القناعة غير المعبَّر عنها من قبل الفرد، وبالتالي لا يكون هناك مجال للدولة لقمعها[2]، كما تختلف عن حرية الإعلام التي تعرّف على أنها إمكانية إبلاغ الآخرين بالأخبار أو الآراء عبر وسائل الإعلام[3].

وعليه، وللإجابة على الإشكال المطروح، لن يتم التركيز في هذه الدراسة على جرائم الإعلام فقط، بل على كافة الجرائم المرتبطة بحرية التعبير الماسّة بحقوق وحريات الأفراد، وسيتم تقسيم الدراسة إلى قسمين رئيسيين: يتم التعرّض في الأول منهما إلى مدى مواءمة الأحكام المجرّمة لأفعال التحريض على الفسق والمساس بالشرف والاعتبار للتطور الإلكتروني الحاصل،

---

[1]. حسن ملحم، محاضرات في نظرية الحريات العامة، ديوان المطبوعات الجامعية، الجزائر، طبعة 1980، ص 72.

[2]. Patrick. WACHMSANN, Libertés publiques, Dalloz, 4eme édition, Paris, 2002, p.429.

[3]. ماجد راغب الحلو، حرية الإعلام والقانون، منشأة المعارف، الإسكندرية، 2006، ص 07.

قبل التعرض في القسم الثاني إلى مدى مواءمة الأحكام الجزائية ذات الصلة بانتهاك حرمة الحياة الخاصة للتطور المذكور. حيث سيتم الخوض خاصة في تحليل عنصر العلانية، بِاعتباره حلقة الوصل بين نصوص التجريم والعقاب ووسائل الاتصال الإلكترونية.

ولأجل ذلك كله، ستتم الاستعانة في هذه بالمنهج الوصفي لاستعراض ووصف الأحكام القانونية ذات الصلة، وبالمنهجين الاستدلالي والتحليلي لتحليل بعض الأحكام وإستخلاص النتائج منها بطريق القياس، وكذا بالمنهج المقارن بين الفينة والأخرى لأجل الوقوف على الحلول التي تبنتها بعض التشريعات المقارنة في ذات المسألة.

المبحث الأول:

مدى مواءمة النصوص المجرِّمة لأفعال التحريض على الفسق والمساس بالشرف والاعتبار للتطور الإلكتروني

تعتبر جرائم تحريض القصّر على الفسق وفساد الأخلاق وجرائم المساس بالشرف والاعتبار من أبرز مظاهر الممارسة التعسفية لحرية التعبير عن الرأي. ولأن التطور الكبير في وسائل الاتصال الإلكتروني قد ضاعف من نطاق هذه الجرائم وزاد في أثرها، فسيكون من المفيد معرفة مدى مواكبة الأحكام العقابية التي جاء بها المشرع الجزائري لمواجهة الجرائم المذكورة للتطور الإلكتروني، وهو ما سنتعرض إليه فيما يلي:

المطلب الأول: مظاهر مواءمة النصوص المجرِّمة لتحريض القصّر على الفسق والدعارة للتطور الإلكتروني

تعتبر جريمة تحريض القصّر على الفسق وفساد الأخلاق من أكثر الجرائم المتصلة بحرية التعبير والشائع اِرتكابها بطريق وسائل الاتصال الإلكتروني. وتختلف أحكام هذه الجريمة ونطاق التجريم فيها بحسب المدى الذي تأخذه فكرة النظام والآداب العامة في الدولة. فهنالك دول تميل إلى فسح مجال حرية الإنتاج السينمائي -وهي أحد أنماط حرية التعبير- ولا تضع إلا بعض القيود الخفيفة على الأفلام السينمائية ذات المحتوى الإباحي أو الماسة بالأخلاق، وطبيعي أن يضيق في هذه الدول نطاق تجريم فعل تحريض القصر على الفسق وفساد الأخلاق. وفي المقابل، هنالك دول أخرى تميل إلى تقديس فكرة النظام العام والآداب العامة وحظر -أو على الأقل تشديد- الرقابة على المنتجات السينمائية الماسة بالأخلاق، وهنا سيتسع نطاق تجريم تحريض القصّر على الفسق والدعارة.

والواقع أن الجزائر تدخل ضمن الصنف الثاني من الدول، حيث ينص قانونها للعقوبات في مادته 342 على أن "كل من حرّض قصّرًا لم يكمِلوا التاسعة عشرة ذكوراً أو إناثاً على الفسق أو فساد الأخلاق أو تشجيعهم عليه أو تسهيله لهم، وكل من ارتكب ذلك بصفة عرضية بالنسبة لقصّر لم يكمِلوا السادسة عشرة يعاقب بالحبس من خمس سنوات إلى عشر سنوات وبغرامة من 20.000 إلى 100.000 دج. ويعاقب على الشروع في اِرتكاب الجنح المشار إليها في هذه المادة بالعقوبات ذاتها المنصوص عليها بالنسبة لتلك الجنح".

والواضح من المادة أعلاه أن الركن المادي في الجريمة موضوع التجريم يتحقق بفعل التحريض على الفسق أو فساد الأخلاق أو التشجيع عليه أو تسهيله للقصّر. والتحريض هو الإغراء أو الإثارة، أو هو توجيه النشاط الإجرامي نحو الغير توجيهاً من شأنه دفعه إلى ارتكاب جريمة معيّنة، وذلك بخلق الفكرة الإجرامية أو إثارتها أو تعزيزها لديه[1]. أما التّسهيل فيقصد به تقديم يد المساعدة للقصّر بشكل يؤدي إلى النتيجة ذاتها، وهي ولوجهم إلى عالم الفسق والدعارة. ويجب أن يوجّه السلوك الإجرامي المشار إليه أعلاه إلى القصّر الذين لم يكملوا تسعة عشر (19) سنة كاملة ذكوراً كانوا أم إناثًا، كما يجب أن يستهدف تلبية شهوات الغير وليس تحقيق شهوات ونزوات شخصية للمحرِّض، وهو ما أكده قرار المحكمة العليا بتاريخ 1982/02/02 والذي جاء فيه: "...تشترط المادة 342 لتطبيقها أن يقدِم المتهم على تحريض القاصر على الفساد أو الفسق إرضاءً لشهوات الغير لا تحقيقاً لرغبته الشخصية..."[2].

ولكن ما يلاحظ من نص المادة أعلاه هو عدم اِشتراطها لتحقق النتيجة الإجرامية، فالشروع في الفعل المجرّم في حد ذاته معاقبٌ عليه، كما أنها لا تشترط العلانية في إتيان السلوك المجرّم، لتنضاف إلى هاتين الخاصيتين خاصية أخرى نصت عليها المادة 345 وهي عدم اِشتراط وقوع الأفعال المجرّمة داخل أرض الوطن، وهو ما يسمح -نظرياً- بمتابعة المسؤولين عن المواقع الإباحية ومذيعي المواد السمعية البصرية الخليعة من خارج الوطن.

ومن ثم، فإن الجريمة المنصوص عليها في المادة 342 أعلاه تتحقق بمجرد اِقتران الركن المادي سالف الإشارة أعلاه بالركن المعنوي الذي يختلف هنا بحسب سن القاصر الذي وُجِّه

---

[1] . عبد الله إبراهيم محمد المهدي، ضوابط التجريم والإباحة في جرائم الرأي، دار النهضة العربية، الطبعة الأولى، القاهرة، 2005، ص 159.

[2] . غ ج 2، المحكمة العليا، قرار 1982/02/02. أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، منشورات بيرتي، الجزائر، طبعة 2007-2008، ص 157.

إليه السلوك، بحيث أنه إذا كان عمر القاصر أقل من ستة عشر (16)، فهنا تتحقق الجريمة ولو وقع السلوك الإجرامي بشكل عرضي، أي بدون أن تتّجه إرادة الجاني إلى إتيانه. أما إذا كان سن القاصر أكبر من ذلك فيشترط في هذه الحالة توافر القصد الجنائي العام، بمعنى أن تتّجه إرادة الجاني إلى إتيان السّلوك المادي المكوِّن للجريمة، مع علمه الكامل بأنه يقوم بتحريض من لم يبلغ تسعة عشر (19) سنة كاملة على الفسق وفساد الأخلاق أو يشجعه عليه أو يسهله له، وهو ما يؤكِّده قرار المحكمة العليا الصادر بتاريخ 27 يناير 1987 والذي جاء فيه: "...وتشترط أيضاً القصد الجنائي الذي يتوافر متى علِم الجاني بأنه يتعامل مع قاصر من جهة وأنه أقدم عمداً على إفساده إرضاء لشهوات الغير..."[1].

في محصلة القول، إن نص المادة 342 قابلٌ للتطبيق بصرف النظر عمّا إذا كان السلوك المجرّم علنياً أم لا، وبصرف النظر عن مكان اِرتكابه، وهو ما يجعل المادة منسجمة إلى حد بعيد مع التطورات التي يعرفها العالم وتعرفها البلاد في المجال الرقمي. لكن ما يلفت اِنتباهنا هو عدم نص المشرع على أي عقوبة موجّهة للشخص المعنوي فيما لو اُرتكب الفعل من قبل أحد ممثليه ولحسابه، وذلك أمر نعتبره غريباً، لاسيما وأن التطور الرقمي كشف عن وجود العديد من المواقع والقنوات الإعلامية تنشط في شكل مؤسسات نظامية وتشتغل في المجال الإباحي. بل إن الأفعال المجرّمة قد يتصور اِرتكابها حتى من قبل هيئة إعلامية خاضعة للقانون الجزائري، وفي هذه الحالة، فالعقوبات الإدارية المتواضعة أصلاً لا نراها كافية لمثل هكذا جرائم ماسة بالأخلاق وبالقيم الإسلامية للمجتمع الجزائري.

بل إننا وفي ظل التطور الرقمي وعدم قدرة أي دولة بما فيها الجزائر على حجب القنوات الفضائية والمواقع الإلكترونية ذات المحتوى الإباحي، نعتقد بأن المادة 345 سالفة الذكر تحتاج إلى مراجعة، ذلك أن صياغتها الحالية تسمح بمتابعة أي أجنبي يَقدُم إلى الجزائر ويكون قد نشر اِنطلاقاً من دولته مواداً إباحية تشجع على الفسق والفجور، وطبعاً من شأن ذلك أن يدخل البلاد في أزمات دبلوماسية لا متناهية بالنظر لكثرة البلدان التي تبيح ممارسة مثل هذه الأنشطة وفق ضوابط قانونية معينة.

وفي ظل القصور النسبي الموضح أعلاه، نعتقد بضرورة تضمين المادة 345 من قانون العقوبات بنداً يشترط توجيه السلوك الإجرامي سالف الإشارة إلى القصر الجزائريين في حال

[1] . غ ج 2، المحكمة العليا، قرار 1987/01/27، ملف 43167. أنظر في ذلك أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، المرجع السابق، ص 157.

وقع السلوك الإجرامي خارج أراضي الوطن، وذلك أسوة بالحل الذي كان قد جرى إعماله بموجب المادة 15 من القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، حيث نصت هذه المادة على منح اِختصاص النظر في الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال إلى المحاكم الجزائرية حتى لو كانت مرتكبة خارج التراب الوطني من قبل شخص أجنبي، وذلك حينما يكون المستهدف منها هو مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

والواقع أن توجيه التحريض للقصّر الجزائريين يمكن اِستنتاجه من خلال الإعلانات الواردة على القنوات والمواقع المعنية ومن خلال أرقام الهواتف المتاحة للمتصلين بهم. ولكن نعتقد كذلك بضرورة مراجعة المادة 12 من القانون رقم 09-04 أعلاه، على النحو الذي يلزم مقدِّمي خدمات الأنترنت بمنع المعطيات المنطوية على مخالفة للنظام العام والآداب العامة، وليس فقط وضع ترتيبات لحصر إمكانية الوصول إلى هذه المعطيات.

ولكننا نعتقد كذلك بضرورة مراجعة المادة 342 على النحو الذي يقر المسؤولية الجزائية للشخص المعنوي فيما لو وقع السلوك الإجرامي من قبل أحد ممثليه ولحسابه.

في المقابل، نلاحظ أن المشرع الإماراتي كان أكثر توفيقاً بشأن هذه المسألة، ذلك أنه وبموجب المادة 47 من المرسوم بقانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات؛ نص على انطباق هذا القانون حتى على الجرائم التي ترتكب خارج الدولة ولكن فقط إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة إلكترونية أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية أو إحدى الحكومات المحلية لإمارات الدولة أو إحدى الهيئات أو المؤسسات العامة المملوكة لأي منهما، بما يفيد بمفهوم المخالفة بأن الجرائم التي ترتكب ضد الأفراد من الخارج أو التي لا ترتكب ضد الأنظمة المعلوماتية والمؤسسات الموجودة في دولة الإمارات لا تخضع للقانون الإماراتي، بل يسري عليها القانون الوطني لمرتكب الجرم، وذلك ما نراه عين الصواب.

ثم إن المشرع الإماراتي كان أكثر تخصيصاً في تجريمه لأفعال التحريض على الفسق والفجور باستخدام شبكة معلوماتية أو إحدى وسائل تقنية المعلومات، حيث نص في المادة 19 من القانون الاتحادي سالف الذكر على توقيع عقوبة السجن والغرامة المتراوحة بين 250 ألف ومليون درهم إماراتي على كل من يرتكب الأفعال المذكورة، مع تشديد العقوبة فيما لو كان

---

[1]. جريدة رسمية عدد 47 الصادرة بتاريخ 16 أوت 2009.

المجني عليه حدثاً لم يكمل الثامنة عشر سنة. وكنا نحبذ لو أن المشرع الجزائري سلك مسلكاً مشابهاً لمسلك نظيره الإماراتي في تخصيص بند خاص بجريمة تحريض القصّر على الفسق في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المطلب الثاني: مدى مواءمة النصوص المجرِّمة للأفعال الماسة بالشرف والاعتبار للتطور الإلكتروني

يمكن تلخيص جرائم التعبير عن الرأي الماسّة بالشرف والاعتبار في جرائم القذف والسب العلني. وعموماً، نقول بأن الأحكام المعاقبة على هذه الجرائم إستطاعت التكيف مع التطور الذي عرفه مجال الإعلام والاتصال الإلكتروني. وسنحاول فيما يلي إبراز مظاهر هذا التكيف.

الفرع الأول: مظاهر مواءمة النصوص المجرِّمة للقذف مع تطور وسائل الاتصال الإلكتروني

يعتبر القذف الموجّه للأفراد من أكثر جرائم التعبير شيوعاً، لاسيما في ضوء التطور الرقمي الذي أدى إلى تنويع وسائل التعبير عن الرأي. وبالنظر لخطورتها على شرف الأفراد وإعتبارهم فقد نص عليها المشرع الجزائري في المادة 296 من قانون العقوبات الجزائري. ووفقاً لهذه الأخيرة يتحقق الركن المادي لهذه الجريمة بكل إدِّعاء بواقعة أو إسنادها إلى شخص المجني عليه تمثِّل اعتداءً على شرفه أو إعتباره، على أن يتم ذلك بشكل علني.

وعليه، فالركن المادي في جريمة القذف مرهون بتوافر أربعة عناصر: فعل الادِّعاء أو الإسناد، أن ينصبّ هذا الادعاء أو الإسناد على واقعة مخلّة بالشرف والاعتبار، أن يكون المستهدف من الفعل محدّداً تحديداً كافياً، وأخيرًا أن يتم ذلك بشكل علني.

والعلانية هي الجهر بالشيء وتعميمه أو إظهاره، أي إحاطة الناس علماً به، وفي جرائم الإعلام يقصَد بها نشر العبارات أو إذاعة الأقوال المجرّمة[1]. وهي تعدّ عنصرًا جوهريًّا في كافة جرائم الصحافة وليس فقط في جريمة القذف، وغيابها ينفي وجود الجريمة حتى ولو توافرت أركانها الأخرى[2]، ولا عجب أن بعض الفقه ذهب إلى حدِّ إلى إعتبارها ركنًا مستقلاًّ بذاته في جرائم الإعلام[3].

---

[1]. خالد مصطفى فهمي، حرية الرأي والتعبير، دار الفكر الجامعي، الإسكندرية، 2009، ص 175. أنظر كذلك طارق سرور، جرائم النشر، دار النهضة العربية، الطبعة الثانية، القاهرة، 2001، ص 13، 14.

[2]. طارق كور، جرائم الصحافة، دار الهدى، الجزائر، 2008، ص 34.

[3]. خالد مصطفى فهمي، المرجع السابق، ص 370. ونشير إلى أن قضاء المحكمة العليا في الجزائر وبموجب القرار الصادر بتاريخ 31 مايو 2000 قد ذهب هو الآخر إلى اعتبار العلانية ركنًا مستقلاً بذاته.

ويتعيّن على قاضي الموضوع إستظهار توافر عنصر العلانية في جريمة القذف، ويبيّن في حكمه طريقة تحقّقها لكي يتسنى للمحكمة العليا مراقبة صحة تطبيق القانون وإلاّ كان حكمه مَعيباً وجب نقضه، وهو ما إنتهى إليه قرار المحكمة العليا بتاريخ 1999/10/19 والذي جاء فيه: "...تتطلّب جنحة القذف توافر العلانية التي يجب إبرازها في القرار وإلاّ كان مشوباً بالقصور..."[1].

والظاهر أن المشرّع الجزائري قد تأثر بنصّ المادة 29 من قانون حرية الصحافة الفرنسي[2]، حين عمِد إلى تعداد طرق ووسائل العلانية في نصّ المادة 296 أعلاه والتي جاء فيها: "...كان من الممكن تحديدها من عبارات الحديث أو الصّياح أو التهديد أو الكتابة أو المنشورات أو اللاّفتات أو الإعلانات موضوع الجريمة...".

والحديث أو القول هو كل ما ينطق به الإنسان من عبارات بِلغات مختلفة ولو كانت مقتضبة[3]. أما الصِّياح فهو نطق الشخص بصوت مرتفع بحيث يستطيع الغير سماعه[4]، ولا تهم نبرة الصوت فقد يتحقق القذف بالصراخ كما قد يتحقق بالغناء[5]. والتهديد حسب بعض الفقه هو توجيه عبارة ما أو ما في حكمها إلى المجني عليه عمداً يكون من شأنها إحداث الخوف عنده من إرتكاب جريمة أو إفشاء أو نسبة أمور خادشة للشرف إذا وجِّهت بالطريقة التي يعاقِب عليها القانون[6]. أما الكتابة فهي حسب بعض الفقه كل ما هو مكتوب أيّاً كان شكله أكان بخطّ اليد أم كان مطبوعاً، وسواء كانت المطبوعات دورية كالصحف أو غير دورية كالكتب[7]. في المقابل،

---

[1] . المحكمة العليا، غ ج م، قسم 02، قرار 1999/10/19ن ملف 198057، غير منشور. نقلاً عن: أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، المرجع السابق، ص 133.

[2] . Jean LARGUIER, Anne-Marie LARGUIER, Droit pénal spécial, Dalloz, 12e édition, Paris, 2002, p 169, 170.

[3] . أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الجرائم ضد الأشخاص والجرائم ضد الأموال، دار هومه، الطبعة الثالثة، الجزائر، 2006، ص 197. أنظر كذلك إيهاب عبد المطلب، جرائم السّب- القذف-الإهانة- البلاغ الكاذب، المركز القومي للإصدارات القانونية، الطبعة الأولى، بدون مكان نشر، 2006، ص 23.

[4] . طارق سرور، المرجع السابق، ص 22.

[5] . المرجع نفسه، ص 22.

[6] . رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، ط 2، القاهرة، دار الفكر العربي، القاهرة، 1985، ص 423.

[7] . طارق سرور، المرجع السابق، ص 23.

يقصد بالمنشورات وفق المفهوم التقليدي كل مطبوع دوريّاً كان أم غير دوري، أما اللاّفتات فهي اللّوحات الإعلانية أو الإشهارية[1]. وليس واضحاً هنا ما إذا كان تعداد طرق العلانية المذكورة قد وردت على سبيل المثال أم الحصر، مثلما ليس هو واضح ما إذا كان مدلول عبارات "الحديث والكّابة والمنشورات والإعلانات" يتّسع ليشمل تلك التي تقع بإحدى وسائل الاتصال الإلكتروني.

ونعتقد بأن القذف قد يقع بإحدى وسائل الإعلام المرئي والمسموع كالإذاعة والتلفزيون، مثلما قد يقع بإحدى وسائل الاتصال الإلكتروني، فتكون العلانية هنا مفترضة. ذلك أنه وعلى الرغم من إغفال المشرّع الجزائري لتبيان ذلك، لا تحقق العلانية في جريمة القذف إلاّ إذا كان في إمكان عدد غير محدّد من الناس الاطّلاع على الادعاء أو مشاهدته، وهو ما تحققه وسائل الاتصال التي ذكرناها. وبذلك نقول بأن النص المجرِّم لفعل القذف يبقى منسجماً مع التطورات الحاصلة في ميدان الاتصال الرقمي، خاصة وأنه يترك لقاضي الموضوع كامل السلطة التقديرية في تحديد الوقائع التي على ضوئها يحكم بتوافر علانية القذف أو بانتفائها[2].

الفرع الثاني: مظاهر إنسجام النصوص المجرِّمة للسب العلني مع تطور وسائل الاتصال الإلكتروني

بخلاف جريمة القذف، نلاحظ أن المشرع الجزائري لم يدرج في المادة 297 من قانون العقوبات ما يفيد إشتراط العلنية في جنحة السب، حيث إقتصرت المادة على تعريف هذه الجنحة فجاء في نصها: **"يعد سبّاً كل تعبير مشين أو عبارة تتضمّن تحقيراً أو قدحاً لا ينطوي على إسناد واقعة"**[3]، في حين إقتصرت المادتان 298 مكرر و299 على تحديد عقوبة السب بصرف النظر عن الوسيلة المستعملة فيه.

والمراد بالسّبِّ إلصاق صفة أو لفظ جارح أو مشين بشخص معيّن، وهو بذلك يتّفق مع القذف في مساسه بشرف المجني عليه أو إعتباره، غير أن الاختلاف بينهما يكمن في كَوْن القذف ينطوي على ادِّعاء بواقعة محدّدة ماسّة بشرف المجني عليه أو إعتباره أو إسنادها إليه، خِلافاً للسّبِّ

---

[1] . محمد هاملي، آليات إرساء دولة القانون في الجزائر، رسالة دكتوراه علوم في القانون العام، جامعة تلمسان، 2012، ص 440.

[2] . طارق كور، المرجع السابق، ص 42، 43.

[3] . وهو تقريبًا نفس ما جاءت به المادة 29 من قانون حرية الصحافة الفرنسي، والتي عرّفت السّب بأنه كل تعبير مهينٍ أو شتائم أو قدح لا يتضمن إسناد واقعة معينة. أنظر في ذلك أحمد جلال محمود حسن، حرية الرأي في الميدان السياسي في ظل مبدأ المشروعية، رسالة دكتوراه في الحقوق، كلية الحقوق، جامعة الإسكندرية، بدون سنة مناقشة، ص 325.

الذي يتحقق بمجرّد لصق بعض العبارات أو الألفاظ التي تقلِّل من قدره دون أن يتضمّن الفعل إسناد واقعة معينة[1].

وفي كل الأحوال، ليس في تعريف السب ما يفيد اِشتراط وقوعه بشكل علني حتى نقول بأن المادة 297 جاءت كافية ووافية، فشرط العلانية غير مستنتج من هذه المادة، وإنما هو مستنتج من نص المادة 463 فقرة 2 من ذات القانون، والتي نصت على معاقبة كل من يبتدر أحد الأشخاص بألفاظ سباب غير علنية دون أن يكون قد اِستفزه. فبمفهوم المخالفة، طالما كانت العقوبة المنصوص عليها في المادة 463 أعلاه خاصة بالسب غير العلني، فإن ما عداه من سب -ونقصد هنا ذلك المنصوص عليه في المادة 297- يكون علنياً.

ومنه، فإن المشرِّع الجزائري ميّز بين جريمة السّبِّ العلني وجريمة السّبِّ غير العلني، فالأولى وهي المنصوص عليها في المادة 297 أعطاها وصف الجنحة لأنها أكثر وَقعاً على المجني عليه بسبب علنية الفعل المجرّم، أمّا التي نص عليها في المادة 463 فقرة 2 من قانون العقوبات فأعطاها وصف مخالفة.

ولمّا كان شرط العلانية مستنتجاً ضمنياً ولم توضح أشكاله، فيكفي في جنحة السب أن تقع بإحدى وسائل العلانية أيّاً كان شكلها. بمعنى أنها قد تتحقق بطريق القول أو بطريق الكتابة، كما قد تحقق بطريق النشر في وسائل الإعلام السمعي البصري وحتى في وسائل الاتصال الإلكتروني الحديثة. وذلك يجعل النصوص المجرِّمة هذه الجنحة مواكبة لأي تطور قد يحصل في مجال الإعلام والاتصال، بما في ذلك الإلكتروني. وعموماً، يبقى لقاضي الموضوع كامل السلطة التقديرية في تحديد الوقائع التي على ضوئها يحكم بتوافر العلانية أو بانتفائها.

وننوِّه إلى أنه على الرغم من عمومية نص المادتين 296 و297 أعلاه، إلاّ أن المشرع الجزائري عزّزهما بنص خاص ضمّنه في المادة 54 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث نصت هذه الأخيرة على معاقبة كل من ينشر معلومات تنطوي على مساس بحقوق الأشخاص وشرفهم وسمعتهم بالحبس من سنتين إلى خمس (5) سنوات وغرامة من 200 ألف إلى 500 ألف دج[2]. وما يستوقفنا في نص هذه المادة هو نصها على أن تطبيق العقوبة المذكورة لا يحول دون تطبيق

---

[1] Patrick WACHSMANN, op, cité, p 445..

[2] . المادة 54 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

العقوبات الأشد والمنصوص عليها في التشريع الساري المفعول، في حين أنه بالرجوع إلى المادتين 298 و298 مكرر من قانون العقوبات نجدهما تقرّران –على التوالي- عقوبة أخف لفعلي القذف والسب العلني؛ حيث تمثل عقوبة القذف في الحبس المتراوح من شهرين إلى ستة (6) أشهر والغرامة من 25 ألف إلى خمسين (50) ألف دج، بينما تمثل عقوبة السب العلني في الحبس من خمسة (5) أيام إلى ستة (6) أشهر والغرامة من 10 آلاف دج إلى 25 ألف دج. ومن ثم فإن التساؤل الذي يطرح في هذا الصدد هو: في حال ارتكاب جريمة قذف أو سب في حق أحد الأفراد بإحدى الوسائل الإلكترونية، هل تطبق العقوبة المنصوص عليها في المادتين 298 و298 مكرر من قانون العقوبات؟ أم تطبق العقوبة المنصوص عليها في المادة 54 من القانون رقم 18-07 والتي تصل إلى الحبس لمدة خمس سنوات؟

إن الإجابة على التساؤل المذكور تقتضي تسليط الضوء على المجرم الذي تقصده المادة 54 أعلاه، هل هو الشخص المحترف المؤتمن على المعطيات الإلكترونية الشخصية للفرد والمسؤول عن معالجة هذه المعطيات؟ أم هو كل فرد يقوم بنشر المعطيات على النحو الذي يمس بسمعة الأفراد واِعتبارهم؟

في هذا الصدد، وعلى الرغم من أن المادة السادسة من القانون رقم 18-07 أعلاه اِستثنت من مجال تطبيق هذا الأخير عمليات المعالجة التي لا تجاوز الاستعمال الشخصي أو العائلي بشرط عدم إحالتها إلى الغير أو نشرها، بما يفيد بأن عمليات نشر المعطيات الشخصية الممارسة في إطار الاستعمال الشخصي غير مشمولة بالاستثناء، ومن ثم تنطبق عليها أحكام القانون رقم 18-07، فإننا نعتقد في الواقع بأن الأحكام الجزائية الواردة في القانون رقم 18-07 لا تخص الأفراد العاديين، وإنما تخص الأشخاص الطبيعية والمعنوية التي –بحكم نشاطها- تستطيع الوصول وبشكل قانوني للمعطيات الشخصية للأفراد، لاسيما وأن هذا القانون يمنع إطلاع الغير على المعطيات الشخصية إلاّ لدواعي إنجاز الغايات المرتبطة مباشرة بمهام المسؤول عن معالجة هذه المعطيات ومهام هذا الغير الذي يتم اِطلاعه، وبعد الموافقة المسبق للشخص المعني[1]، كما يشترط ضمن أحكامه اِستيفاء إجراء التصريح لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو الحصول على ترخيص منها، لأجل نشر المعطيات الشخصية للأفراد[2]، وهو ما لا يمكن تصور تطبيقه على الأفراد العاديين، وإلاّ لاحتاجت السلطة المذكورة لجيش من الموظفين

[1]. المادة 7 فقرة 3 من القانون رقم 18-07 أعلاه.

[2]. أنظر المواد 12، 13، 17 و21 من القانون رقم 18-07 أعلاه.

يعملون دون انقطاع لأجل تلقي التصريحات ومنح وصولات الاستلام والتراخيص التي يفرضها القانون عند كل عملية نشر لمعطيات شخصية.

وفي ضوء عدم وضوح النص، وعدم وضوح تعريف الشخص المسؤول عن معالجة معطيات الأفراد، نعتقد بأن المشرع قد خانة التوفيق في صياغة المادة السادسة من القانون رقم 18-07، حينما اشترط في المعالجة الموجهة للاستعمال الشخصي أو العائلي ألاّ تكون موضوع نشر أو إحالة للغير، فلو أنه إستثنى جميع حالات النشر التي يقوم بها الأفراد العاديون لكان أفضل، ولأمكن حينها تطبيق القواعد العامة المنصوص عليها في قانون العقوبات على هذه التجاوزات، بينما تكون العقوبة المغلّظة المقررة في المادة 54 أعلاه موجّهة فقط للشخص المحترف المسؤول عن المعالجة الإلكترونية حين اِرتكابه للتجاوز.

في المقابل، نلاحظ أن المشرع الإماراتي كان أكثر وضوحاً حينما قرّر وبشكل صريح في المادة 20 من القانون الاتحادي رقم 5 لسنة 2012 تجريم سب الأشخاص واِزدرائهم باستخدام شبكة معلوماتية أو أية وسيلة تقنية معلومات، وقرّر لذلك عقوبة الحبس والغرامة التي تتراوح من 250 ألف إلى 500 ألف درهم إماراتي، أو بإحدى العقوبتين المذكورتين[1].

المبحث الثاني: مدى مواءمة الأحكام الجزائية المتعلقة بحماية حرمة الحياة الخاصة للتطور الإلكتروني

على الرغم من أن حق المواطن في حرمة حياته المواطن تمت كفالته دستوراً منذ تبني دستور سنة 1976[2]، ليتم تكريسه فيما بعد في الدساتير اللاحقة[3]، إلاّ أن المشرع الجزائي الجزائري وبِاستثناء الأحكام التي أوردها في قانون العقوبات لحماية سرية المراسلات تأخر في توفير الأحكام الردعية لحماية باقي عناصر الحياة الخاصة إلى غاية نهاية سنة 2006، أين صدر القانون رقم 06-23[4]. ولكنه وعلى غرار جلِّ التشريعات المقارنة، أحجم عن وضع تعريف للحياة الخاصة واِكتفى ببيان الأحكام التجريميّة والعقابية لفعل الاعتداء الذي قد يطالها.

---

[1]. فيصل كامل نجم الدين، واقع الجريمة الإلكترونية في مواقع التواصل الاجتماعي -الحماية النظامية في دول مجلس التعاون الخليجي- المجلة الدولية للاتصال الاجتماعي (تصدر عن جامعة عبد الحميد بن باديس -مستغانم)، المجلد 5، العدد 4-2018، ص 21، 22.

[2] . المادة 49 من دستور الجزائر لسنة 1976.

[3] . المادة 37 من دستور الجزائر لسنة 1989 والمادة 39 من دستور الجزائر لسنة 1996.

[4] . القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات، جريدة رسمية عدد 84 الصادر بتاريخ 24 ديسمبر 2006.

والواقع أن مسألة وضع تعريف جامع للحياة الخاصة أثارت اِنقسام الفقه والقضاء على حدٍّ سواء. فبالنسبة لهذا الأخير ذهبت بعض الأحكام إلى التضييق من نطاق الحياة الخاصة وحصرها في الحياة الزوجية أو العاطفية فقط، في حين ذهبت أحكام أخرى إلى التّوسيع من نطاقها ليشمل -إضافة إلى الحياة الزوجية والعاطفية- بعض الوقائع والأحداث المتعلّقة بحياة الفرد[1].

أما الفقه فقد اِنقسم بدوره بين فريق اِختار تعريف الحياة الخاصة بشكل إيجابي وآخر اِختار تعريفها بشكل سلبي. فبالنسبة للفريق الأول ذهب جانبٌ من الفقه الأمريكي إلى تعريف الحق في الحياة الخاصة على أنه الحق في الخلوَة وفي عدم تعكير صفواها[2]. في حين عرّفه جانبٌ آخر بأنه رغبة الإنسان في الوِحدة والألفة والتخفّي والتحفظ[3]. ولم يحِد الفقه الفرنسي عن هذا الاتجاه عندما اعتبر البعض منه بأن الحق في الحياة الخاصة هو حق الشخص في أن يترَك في هدوء وسكينة[4].

ونشير إلى أن هذه التعريفات قد تعرّضت للنقد بسبب عدم تقديمها لمعيار قانوني دقيق لتحديد المقصود بالحياة الخاصة[5]. وأمام هذا الوضع ذهب جانبٌ من الفقه إلى وضع تعريف سلبي للحياة الخاصة بالقول بأن هذه الأخيرة هي كل ما لا يعتبَر من قبيل الحياة العامة للشخص[6]. وعُرِّفت الحياة العامة بأنها كل ما يكون من الجائز نشره على الناس من نشاط الشخص أو أحواله لاِتّصاله بحياتهم أو لانكشافه أمامهم[7]. غير أن هذا التعريف يثير بعض الصعوبة لكون الحياة

---

[1] . عبد الله إبراهيم محمد المهدي، المرجع السابق، ص276.

[2] . نصر الدين مروك، الحق في الخصوصية، مجلة النائب، العدد الثاني، 2003، صادرة عن المجلس الشعبي الوطني، الجزائر، ص 18.

[3] . محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، دار النهضة العربية، القاهرة، 2005، ص 115.

[4] . أشرف توفيق شمس الدين، الصحافة والحماية الجنائية للحياة الخاصة، دار النهضة العربية، الطبعة الأولى، القاهرة، 2007، ص 19.

Jean MORANGE, Droits de l'homme et libertés publiques, 5^{e} édition, PUF, Paris 2000, p.177.

[5] . نصر الدين مروك، المرجع السابق، ص 18.

[6] . محمد عمر حسين، حرية الصحافة في مصر ودور القضاء في حمايتها (دراسة مقارنة)، رسالة دكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 1999، ص 426..

[7] . محمد الشهاوي، المرجع السابق، ص 107.

العامة للسياسي مثلاً وثيقة الصِّلة بحياته الخاصة[1]. لِذا لجأ بعض الفقه إلى اعتماد معيار "المصلحة العامة" التي تقتضي إعلام الجمهور بالأخبار كمعيار للتمييز بين الحياة الخاصة والحياة العامة للفرد[2]، في حين لجأ البعض الآخر إلى اعتماد معيار "شعور الفرد بالحياء تجَاه أُلفَة حياته" كحدٍّ فاصل بين حياته العامة وحياته الخاصة، فمتى بدأ هذا الشعور في الظهور يبدأ نطاق الحياة الخاصة وتنتهي الحياة العامة[3]. لكن مع ذلك لم يسلم هذا الرأي من النقد على أساس أن المعيار المحدِّد للحياة العامة هو معيار مرن قد يتّسع ليشمل حالات كثيرة يشكِّل فيها النشر اعتداء على الحياة الخاصة. كما أن عناصر الحياة العامة لا تزال في حاجة إلى تحديد والحياة المهنية والوظيفية لا تعتبر من عناصر الحياة العامة في مطلق الأحوال[4]، فضلاً عن أن الشعور بالحياء قد يختلف من شخص لآخر.

وعليه، يمكن القول بأن وضع تعريف جامع للحق في الحياة الخاصة أمرٌ بالغ الصعوبة نظراً لنسبية الحياة الخاصة سواء من حيث الأشخاص أو من حيث الزمان والمكان[5]، إضافة إلى تأثر نطاق الخصوصية بالنطاق الذي تمنحه بعض المجتمعات لبعض القيم ومنها حرية الصحافة والحق في الإعلام، فيضيق نطاق الحق في الخصوصية أو يتّسع بحسب نطاق الحرية الذي تتمتع به الصحافة. وقد أكّد مؤتمر اليونسكو المنعقد بباريس في يناير من سنة 1970 على أنه من الصعوبة بمكان تعريف جوهر مفهوم الخصوصية تعريفاً عالميّاً، نظراً لأن الخصوصية مسألة نسبية مرتبطة بالثقافة والمحتوى الاجتماعي والاقتصادي لكل دولة من الدول[6].

وأمام هذا الوضع اتجه الفقه إلى العدول عن وضع تعريف للحياة الخاصة، وحاول بالمقابل وضع قائمة بالقيم التي تحميها وتغطِّيها فكرة الحياة الخاصة مسترشداً في ذلك بتطبيقات القضاء، وتشمل[7]: الحياة العاطفية والزوجية والعائلية للشخص؛ الذمة المالية؛ الحالة الصحية والرعاية

---

[1] . جمال الدين العطيفي، حرية الصحافة وفق تشريعات جمهورية مصر العربية، مطابع الأهرام، الطبعة الثانية، القاهرة، 1974، ص 142.

[2] . أشرف توفيق شمس الدين، المرجع السابق، ص 28.

[3] . محمد الشهاوي، المرجع السابق، ص 106.

[4] . Louis FAVOREU et autres, Droit des Libertés fondamentales, Dalloz, 2ème édition, Paris 2000, p 411.

[5] . محمد عمر حسين، المرجع السابق، ص 437.

[6] . مروك نصر الدين، المرجع السابق، ص 23.

[7] . محمد الشهاوي، المرجع السابق، ص 120.

الطبية، محل الإقامة ورقم الهاتف الشخصي، حرمَة جسم الإنسان بما في ذلك صورته، الحالة النفسية والعقلية للإنسان، حرمة المسكن ومراسلات الشخص...

فحقيقة إن الحياة الخاصة للأفراد يمكن أن تكون محلاً لأخطر الاعتداءات من قبل الغير، وتزداد هذه الخطورة ويتّسع أثرها إذا وقعت بالطريق الإلكتروني، بالنظر للمدى الذي يمكن أن تصل إليه التسجيلات والصور المنشورة بالطريق الإلكتروني، ونستحضر هنا واقعة سرقة معطيات إلكترونية ذات طبيعة جنسية تعود للمترشح لمنصب عمدة باريس "B.Griveaux" ونشرها في مواقع التواصل الاجتماعي، الأمر الذي أدى إلى الحط بسمعة الضحية ودفعه للاِنسحاب من سباق الترشح للمنصب المذكور. إلا أن فرنسا تحوز على ترسانة قانونية معدة سلفاً لمثل هذه التجاوزات، ونعني هنا القانون "لأجل جمهورية رقمية" الصادر سنة 2016 تحت رقم 2016-1321، والذي تم الاستناد إليه لتحريك متابعة جزائية ضد مرتكب الجرم أعلاه. فالقانون المذكور خصّص المواد من 54 إلى 67 لحماية الحياة الخاصة للأفراد.

في المقابل، إذا ما بحثنا في المنظومة القانونية الجزائرية سنجد بأن المشرع الجزائي الجزائري -وكما سبق وأشرنا- تأخر إلى غاية نهاية سنة 2006 لسن قانونٍ يجرِّم الاعتداءات على الحياة الخاصة بكل أشكالها، بعدما كان سابقاً قد اِكتفى بتجريم انتهاك سرية المراسلات وإفشاء السر المهني، قبل أن يطعمه بالقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وسنحاول فيما يلي تسليط الضوء على مدى مواكبة النصوص التجريمية التي جاء بها المشرع الجزائري للتطور الرقمي، بالتعرض بداية إلى الأحكام العقابية الخاصة بجرائم نشر المراسلات الخاصة، وتلك الخاصة بجرائم إفشاء الأسرار المهنية ونشرها، قبل التعرض فيما بعد إلى جرائم نشر متعلّقات الحياة الخاصة بشكل عام.

المطلب الأول: مدى مواكبة الأحكام التجريمية لنشر المراسلات والأسرار المهنية للتطور الإلكتروني

سبق وأشرنا إلى أن الفقه والقضاء قد عجزا عن وضع معيار حاسم لتعريف الحياة الخاصة للإنسان، ليستقر الاجتهاد على وضع قائمة بالقيم التي تدخل ضمن مفهوم الحياة الخاصة. كما سبق

Voir aussi: Micheline DECKER, Aspects internes et internationaux de la protection de la vie privée en droit français, allemand et anglais, Thèse pour obtenir le grade de docteur, Université Panthéon- Assas (France), 2000, p 489, 490.

وذكرنا بأن المراسلات الخاصة تدخل ضمن هذا المفهوم، مثلما تدخل فيه الأسرار المتحصل عليها بحكم المهنة. في هذا الصدد، نلاحظ أن المشرع الجزائي كان قد أدرج أحكاماً تجرِّم وتعاقب على انتهاك سرية المراسلات وإفشاء السر المهني، لكن ما يهمنا في هذه الأحكام هو مدى إحاطتها ببعض الممارسات التعسفية لحرية التعبير، وكذا مواكبتها للتطور الإلكتروني الحاصل.

الفرع الأول: مدى مواءمة الأحكام المجرِّمة لنشر مضمون الرسائل والمراسلات للتطور الإلكتروني

نقصد بالرسائل والمراسلات هنا جميع المراسلات المكتوبة أو المصورة أو المسموعة و/أو المرئية، سواء تمت بطريق الرسائل البريدية التقليدية، أو بطريق المواصلات السلكية أو الإلكترونية. ولأن الممارسة التعسفية وغير المسؤولة لحرية التعبير قد تطال حرمة هذه الرسائل أو المراسلات، فقد حفّها المشرع بأحكام جزائية لحمايتها، كانت آخرها المادة 164 من القانون رقم 18-04 المتعلق بالبريد والمواصلات الإلكترونية. حيث نصت هذه الأخيرة على توقيع عقوبة الحبس من سنة واحدة إلى خمس (5) سنوات والغرامة من 500 ألف إلى 1 مليون دج، ضد كل من ينتهك سرية المراسلات التي تتم بطريق البريد أو الاتصالات الإلكترونية أو يقوم بإفشاء مضمونها أو نشره أو إستعماله دون الحصول على ترخيص بذلك من المرسل أو المرسل إليه أو يخبر بوجودها.

وواضحٌ من المادة أعلاه أن الركن المادي للجريمة أعلاه يتحقق من خلال عدة سلوكات مجرّمة، أحدها يتمثل في نشر المراسلات الإلكترونية دون إذن المرسل أو المرسل إليه. ولأن المادة لم تحدد سبل النشر هنا، فيحال في ذلك إلى مختلف الوسائل التي قد يتم بها ومنها الأنترنت التي تعتبر في الواقع أخطر الوسائل، بالنظر للمدى الذي قد يبلغه الأثر الإجرامي بواسطتها، والذي يصعب التحكم فيه ومحو آثاره.

فإذا ما إذا كان الشخص المعنوي ضليعاً في الجرم المرتكب؛ بأن كان السلوك المادي قد أُرتكب من قبل أحد ممثليه الشرعيين ولحسابه، فهنا توقع عليه ذات العقوبات المقرّرة في قانون العقوبات[1]، والتي تتدرّج من الغرامة من مرة واحد إلى خمسة أضعاف تلك الموقعة على الشخص الطبيعي، لتصل إلى حد الغلق المؤقت أو الحل[2].

---

1 . أنظر المادة 187 من القانون رقم 18-04 المحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية.

2 . المادة 18 مكرر من قانون العقوبات.

وعليه، يمكن القول بأن القانون رقم 18-04 أعلاه قد سد النقص الذي اِعترى أحكام المادتين 137 و303 من قانون العقوبات[1]، فنطاق التجريم الذي تشمله المادتان المذكورتان قاصر على أفعال فض وإتلاف مراسلات الغير وإذاعة محتوى البرقيات، ولا يشمل أفعال نشر هذه المراسلات، وفوق ذلك فالعقوبات المنصوص عليها في المادة 137 لا تخص إلا أعوان الدولة وموظفي البريد، بينما المادة 303 تشترط توافر سوء النية لدى الفاعل. كما ينبغي القول بأن القانون رقم 18-04 قد سد النقص الذي كان يطبع القانون رقم 2000-03، ذلك أن هذا الأخير لم يتحسّب لجرم نشر المراسلات الإلكترونية، واِكتفى في مادته 127 بتجريم انتهاك سرية الرسائل البريدية والمراسلات التي تتم بطريق المواصلات السلكية واللاسلكية[2]، دونما إشارة إلى أفعال نشر هذه المراسلات، وهو الأمر الذي تصدّت له المادة 164 من القانون رقم 18-04 أعلاه.

الفرع الثاني: مدى اِنسجام النصوص المجرِّمة لإفشاء السر المهني مع التطور الحاصل في المجال الإلكتروني

لقد تم النص على جريمة إفشاء الأسرار في المادة 301 من قانون العقوبات الجزائري، حيث جاء في هذه الأخيرة: "يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 20.000 إلى 100.000 دج الأطباء والجرّاحون والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أُدلي بها إليهم وأفشوها في غير الحالات التي يوجِب عليهم فيها القانون إفشاءها ويصرّح لهم بذلك...".

[1] . تنص المادة 137 من قانون العقوبات على أنه: "كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن المصلحة البريد يقوم بفض أو اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اِختلاسها أو إتلافها يعاقب بالبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30 ألف إلى 500 ألف دج. ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق يختلس أو يتلف برقية أو يذيع محتواها...". أما المادة 303 من قانون العقوبات فنصت على ما يلي: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر إلى سنة وبغرامة من 25 ألف إلى 100 ألف دج أو بإحدى هاتين العقوبتين فقط".

[2] . لقد كانت المادة 127 من القانون رقم 2000-03 المؤرخ في 5 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية (ج ر عدد 48 لسنة 2000) تقرر (بطريق الإحالة إلى المادة 137 من قانون العقوبات) عقوبة الحبس من ثلاثة أشهر إلى خمس سنوات والغرامة من 30 ألف إلى 500 ألف دج

ويمكننا تعريف هذه الجريمة بأنها تعمّد الإفضاء بسرٍّ من شخص أُؤتمن عليه بحكم عمله أو مهنته وذلك في غير الأحوال التي يوجب فيها القانون الإفضاء أو يجيزه، أو هي الكشف عن واقعة لها صفة السِّرِّ صادر ممّن علم بها بمقتضى مهنته مع توافر القصد الجنائي[1].

والعلانية لا تعتبر شرطاً في جريمة إفشاء السِّرِّ، فتتحقق هذه الأخيرة ولو لم يكشَف السر إلاّ لشخص واحد[2]، بل وتتحقق حتى لو اقتصر الإفشاء على جزء فقط من السِّر[3]. ومن باب أولى فهي تتحقق إذا كان الإفشاء علنيّاً بصرف النظر عن الوسيلة التي يتم بها هذا الإفشاء، ولو كانت وسيلة اِتصال إلكتروني، كما لو تم نشر تعليق أو وثيقة طبية في إحدى مواقع التواصل الاجتماعي أو حتى في إطار محادثة إلكترونية خاصة بين المؤتمن على السر وشخص آخر تنطوي على إفضاء لسر مؤتمن عليه.

ولكن مهما كان، لا يعاقِب القانون على إفشاء السِّرِّ إلاّ إذا تمّ من قِبل شخص مؤتمن عليه بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة[4]. وقد ذكرت المادة 301 أعلاه فئات معيّنة على سبيل المثال وهم الأطباء والجرّاحون والصيادلة والقابلات؛ ثم أردفت "وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة". وطبعاً فالصحفي هو من الأشخاص الملزمين بالسِّرِّ المهني[5].

ويرى الأستاذ رؤوف عبيد أنّ نصّ المادة 310 من قانون العقوبات المصري -والتي تقابِلها المادة 301 من قانون العقوبات الجزائري- ينبغي ألاّ يطبّق على الصحفيّين، لأن رسالة هؤلاء تكمن في نشر الأنباء وليس كتمانها مهما كانت في نظر أصحابها أسرارًا، مادام النشر قد تمّ في حدود القوانين التي تنظِّم الصحافة والنشر[6]. ونعتقد بأن هذا القول مجافٍ للصواب، لأن الصحفي وإن كان يتمتع -مثله مثل أي مواطن آخر- بحرية التعبير عن الرأي، إلاّ أن هذه الحرية ينبغي ألاّ تصل إلى حد البوح بما أُؤتمن عليه الشخص من أسرار، فضلاً عن أن إخلال الصحفي

---

[1] . محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، طبعة سنة 1988، ص 75.

[2] . Jean LARGUIER, Anne-Marie LARGUIER, op, cité, p 148.

[3] . عبد الله إبراهيم محمد المهدي، المرجع السابق، ص 291.

[4] . Remy CABRILLAC et autres, Libertés et droits fondamentaux, 9eme édition, Dalloz, Paris 2003, p 175.

[5] . Jean LARGUIER, Anne-Marie LARGUIER, op, cité, p 143.

[6] . محمود نجيب حسني، المرجع السابق، ص 772.

بالسِّرِّ المهني قد يؤدي إلى الكشف عن مصادره الصحفية، وهو أمرٌ قد يعرِّض هذه الأخيرة إلى المضايقات أو المتابعة الجزائية، وذلك سيدفع الجمهور -ولا شك- إلى النّفور من التعامل مع الصحافة ويزعزع الثّقة في أهلها، ما ينعكس سلباً في الأخير على حقِّ المواطن في الإعلام.

على أن هنالك حالات إستثنائية يكون فيها المؤتمن على سرٍّ ما -ولو كان صحفياً- ملزماً بإفشائه تطبيقاً لمقتضيات القانون، ويتعلّق الأمر بحالة طلب الشخص للشهادة بشأن جريمة إجهاض. فإذا ما تم إستدعاء شخص أمام القضاء للشهادة بشأن الجريمة المذكورة، وجب عليه حينها الحضور لأداء الشهادة تحت طائلة العقوبات التي يقررها القانون في هذا الشأن[1]. ولكن مهما يكن من أمر، فإن الشهادة ولو في جرائم الإجهاض تكون أمام القضاء وليس في الفضاءات الإلكترونية. وحتى إن تمت بمحادثة إلكترونية ففي إطار ما يسمح به القانون وتكون بشكل مغلق لا يحقق العلانية وذيوع السر المؤتمن عليه.

ولما كانت جريمة إفشاء الأسرار لا تتطلب العلانية في الإفشاء، يمكننا القول بأن أي وسيلة تستعمل في هذا الإفشاء، بما في ذلك الوسائل الإلكترونية، تعرض الفاعل إلى العقوبات المنصوص عليها في المادة 301 أعلاه إذا ما إكتملت أركان الجريمة الثلاثة. وهو ما يعني بأن تنظيم المشرع لهذه الجريمة ومن البداية، وطبيعة هذه الجريمة غير المستلزمة لشرط العلانية جعلا أحكامها منسجمة مع التطورات التي يعرفها عالم الاتصال الرقمي، وستظل كذلك ما بقيت العلانية في هذه الجريمة غير مشترطة قانوناً.

ولكن رغم ذلك، كنا نحبذ لو أن المشرع الجزائري خصّص حكماً صريحاً يجرِّم بموجبه فعل إفشاء الأسرار بالطريق الإلكتروني، على نحو ما فعل المشرع الإماراتي بموجب القانون رقم 5 لسنة 2012، حينما نص في المادة 22 على توقيع عقوبة الحبس الذي لا يقل عن ستة (6) أشهر والغرامة والتي تتراوح بين 500 ألف ومليون درهم إماراتي، ضد كل من يقوم باستخدام شبكة معلوماتية أو موقعاً إلكترونياً أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه.

المطلب الثاني: مدى مواكبة الأحكام المجرِّمة لنشر متعلقات الحياة الخاصة للتطور الإلكتروني

تتوزع الأحكام المجرّمة لفعل نشر متعلقات الحياة الخاصة على كل من قانون العقوبات وقانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. وسنحاول

[1]. المادة 301 فقرة 2 من قانون العقوبات الجزائري، والمادة 97 فقرة 2 من قانون الإجراءات الجزائية الجزائري.

فيما يلي تسليط الضوء على مدى مواكبة كلا القانونين للتطور الهائل الحاصل في مجال الاتصال الإلكتروني.

الفرع الأول: مدى مواكبة قانون العقوبات للتطور الإلكتروني فيما تعلق بتجريم نشر متعلقات الحياة الخاصة

في البداية، ينبغي التنويه إلى أنه ليست جميع الاعتداءات التي قد تقع على حرمة الحياة الخاصة هي ذات صلة بالتعبير عن الرأي، فمثلاً جريمة اِلتقاط تسجيل أو نقل المكالمات أو الأحاديث الخاصة أو الصور الشخصية المنصوص عليها في المادة 303 مكرر[1]من قانون العقوبات لا تدخل ضمن هذا المفهوم ما لم تقترن بفعل إذاعة الأحاديث والصور الخاصة ونشرها للجمهور، على الرغم من أنها من أخطر الاعتداءات على الحياة الخاصة، لأن الركن المادي في هذه الجريمة يتحقق بمجرّد قيام الجاني بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو صورة للمجني عليه في مكان خاص بغير إذنه أو رضاه، ودون اِشتراط نشرها للعلن. فإذا ما اِقترنت الأفعال المذكورة بفعل النشر للجمهور، بصرف النظر عن الوسيلة المتبعة في ذلك، فإن الفاعل في هذه الحالة سيكون مرتكباً لجرمين اِثنين، المنصوص عليه في المادة 301 مكرر والمنصوص عليه في المادة 301 مكرر1 والمبين أدناه.

ويقصد بالمكالمات أو الأحاديث الخاصة تلك التي لا يتوقع التنصّت عليها أو تسجيلها لا من الشخص المتحدَّث إليه ولا من غيره[2]، أما اِلتقاط الصورة فيقصد به تثبيتها على مادة ما، وتسجيلها يكون بحفظها بجهاز ما، في حين أن نقلها يكون بإرسالها من مكان لآخر[3].

---

[1] . تنص المادة 303 مكرر من قانون العقوبات الجزائري على ما يلي: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1. بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
2. بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المشار إليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة. ويضع صفح الضحية حداً للمتابعة الجزائية".

[2] . عبد الله إبراهيم محمد المهدي، المرجع السابق، ص 279.

[3] . محمد زكي أبو عامر، قانون العقوبات -القسم الخاص- دار المطبوعات الجامعية، الإسكندرية، 1989، ص 698.

فالجريمة المنصوص عليها في المادة 303 مكرر تحقق بصرف النظر عن نشر المحتوى المسجل، ما اِقترن ركنها المادي بالركن المعنوي الذي يتحقق بدوره باتجاه إرادة الجاني وبسوء نية إلى اِرتكاب الأفعال المكوِّنة للركن المادي للجريمة، مع علمه بأن الأمر يتعلّق بأحاديث شخصية أو سرية أو صور للشخص وهو في مكان خاص، وبأن الضحية لم يأذن له أو يعبر عن رضاه بذلك.

ولكن في كثير من الأحيان، يَعمَد الشخص الذي قام بالتقاط أو تسجيل أو نقل أحاديث شخصية أو صور للغير بغير رضاهم إلى إعلان أو استعمال تلك التسجيلات أو الصور نظير مقابل مادي[1]، لذلك حرصت معظم التشريعات على تجريم ومعاقبة هذه الأفعال، كما هو الحال بالنسبة للمشرِّع الجزائري الذي نصّ على ذلك في المادة 303 مكرر1 من قانون العقوبات[2]، والتي تعاقب كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصّل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر والسالف ذكرها أعلاه.

وطبعاً لحلقة الوصل بين إنتهاك حرمة الحياة الخاصة والتعبير التعسفي عن الرأي تكمن في إطلاع الجمهور على التسجيلات أو الصور أو الوثائق. ويقصد بالوضع في متناول الجمهور بمفهوم المادة؛ إطلاع هذا الأخير على التسجيلات أو الصور أو الوثائق التي تمّ الحصول عليها بالطرق غير القانونية المبيّنة في المادة 303 مكرر. ويقصد بـ "السّماح بأن توضع في متناول الجمهور" تسهيل إعلانها أو قيام الجاني بتقديم المساعدة لمن يقوم بإعلام الجمهور بمضمونها. أما اِستخدام التسجيل أو الصورة أو الوثيقة فيقصَد به إستعمالها بطريقة ما من قبل شخص من أجل الوصول إلى غاية معيّنة، ويستوي أن يتم ذلك بشكل علني أو غير علني[3].

والملاحظ أن المشرع الجزائري -وعلى غرار نظيره الفرنسي- لم يشترط في النشر أو الاستعمال أن يقع بطريقة معينة، ومن ثم فإن الركن المادي للجريمة قد يتحقق بمجرّد نشر أو

---

[1] . أشرف توفيق شمس الدين، المرجع السابق، ص 79. أنظر كذلك محمد الشهاوي، المرجع السابق، ص 279.

[2] . تنص المادة 303 مكرر1 من قانون العقوبات الجزائري على ما يلي: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصّل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون...".

[3] . عبد الله إبراهيم محمد المهدي، المرجع السابق، ص 287. محمد الشهاوي، المرجع السابق، ص 280.

اِستعمال أحاديث أو صور خاصة، بصرف النظر عن الوسيلة المستعملة في ذلك ولو كانت إلكترونية، ما يجعل نص المادة 303 مكرر1 متوائماً مع التطور الذي يعرفه مجال الإعلام والاتصال الإلكتروني. وذلك بديهي برأينا، على إعتبار أن إقرار القانون رقم 06-23 جاء متأخراً مقارنة بدخول تقنية الاتصال الإلكتروني إلى الجزائر.

فوسائل البت الإلكتروني هي أكثر وقعاً على الضحية وأشد ضرراً به، نظراً للمدى غير المحدود الذي يمكن أن تبلغه الأحاديث والصور المنشورة، كمن يقوم بنشر صور شخص آخر في وضعية مخلّة عبر مواقع التواصل الاجتماعي بغية المساس بسمعته، أو بغية تحقيق مآرب سياسية، كما حدث للمترشح لمنصب عمدة باريس في فبراير من سنة 2020 "B.Griveaux". ومن ثم، كان من البديهي، بل من الضروري أن يكون النشر بطريق الإنترنت مشمولاً بمحتوى المادة 303 مكرر 1 أعلاه. وليس شرطاً هنا أن يقع النشر أو الإستخدام من نفس الشخص الذي قام بِالتقاط الصورة أو تسجيل الحديث، فقد يكون مرتكب الجريمة شخصاً آخر.

إلاّ أن ما يلفت اِنتباهنا من نص المادة 303 مكرر1 أعلاه، عدم تجريمه لفعل نشر واِستعمال الأحاديث والصور الخاصة بغير إذن صاحبها أو رضاه. فغياب الإذن أو الرضا مشترط في تجريم تسجيل أو اِلتقاط أو نقل أحاديث أو مكالمات أو صور خاصة للغير، ولكنه غير مشترط في تجريم نشر واِستعمال هذه الأحاديث أو الصور، وفي ذلك نوع من الغرابة والقصور! فلو فرضنا بأن إحدى الفتيات أرسلت لشخص ما صورة لها بلباس غير محتشم بمحض إرادتها بغية إبراز جمالها له وتشجيعه على الزواج منها، ثم قام هذا الأخير بنشر الصورة عبر إحدى مواقع التواصل الاجتماعي، فإن الفعل هنا لن يكون مجرّماً بمنظور المادة 303 مكرر1، لأن الحصول على الصورة ونقلها تم بموافقة المعنية، ولو كان نشرها قد تم من دون موافقتها. كذلك، إن المادة المذكورة لا تتصدى للحالة التي يقع فيها نشر الصور والمعطيات المتعلقة بالحياة الخاصة للأفراد من قبل موظف مؤتمن على تسجيلها أو تنظيمها أو حفظها، كالموظف المكلف بتسجيل وتنظيم المعطيات البيومترية للأفراد، أو الموظف بالشركات المزودة لخدمة الأنترنت...لأن الحصول على المعلومات الشخصية في هذه الحالات تم بالرضا الكامل لصاحبها. وبالتالي فهذه مظاهر للقصور ينبغي تداركها، فهل فعل ذلك القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أو القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي؟ هذا ما سنحاول الإجابة عليه فيما يلي:

الفرع الثاني: مدى مواكبة القانون رقم 18-07 للتطور الإلكتروني فيما تعلق بحماية متعلقات الحياة الخاصة

من خلال الاطلاع على أحكام القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يتبين لنا بأنه لم يتعرّض تماماً لأجه القصور المبينة أعلاه، ولذلك كان يجب اِنتظار صدور القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ليتم سد الفراغ الذي اِعترى المادة 301 مكرر1 من قانون العقوبات –ولو نسبياً- بالعديد من الأحكام الجزائية التي تعاقب على نشر الصور والمعطيات الخاصة بدون موافقة صاحبها، حيث نص هذا الأخير في مادته 55 على معاقبة كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي بدون موافقة من الشخص المعني بالحبس من سنة إلى 3 سنوات وغرامة من 100 ألف إلى 300 ألف دج.

ويقصد بالمعطيات ذات الطابع الشخصي حسب المادة الثانية من ذات القانون، كل معلومة بغض النظر عن دعامتها تتعلق بشخص معرّف أو قابل للتعرّف عليه بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية. أما معالجة هذه المعطيات فيقصد بها -حسب ذات المادة- كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف. ومن ثم، فإن أي نشر أو إتاحة لإحدى المعلومات الشخصية بغير موافقة الشخص المعني تعرِّض الفاعل للعقوبات المذكورة أعلاه.

وحتى لو تم الحصول على موافقة الشخص المعني فإن نشر المعطيات الشخصية يحتاج إلى اِستيفاء واجب التصريح للسلطة الوطنية، وذلك تحت طائلة العقوبة التي تصل إلى الحبس من سنتين إلى خمس (5) سنوات والغرامة من 200 ألف إلى 500 ألف دج[1]، وهي ذات العقوبة

[1] . المادة 56 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المقرّرة لنشر المعلومات المتعلقة بالحياة الخاصة للأفراد وحرياتهم العامة وكذا المتعلقة بحقوق الأشخاص وشرفهم وسمعتهم[1].

أما بالنسبة للمعطيات الحساسة للشخص والتي هي حسب المادة الثانية أعلاه كل معلومة تتعلق بالأصل العرقي أو الاثني أو الآراء السياسية للشخص أو قناعاته الدينية أو الفلسفية أو إنتمائه النقابي أو المتعلقة بصحته، فبالنظر لخطورتها نلاحظ أن المشرع قد قرّر ذات العقوبة المغلظة لمن يقوم بنشرها بدون موافقة صاحبها أو بدون ترخيص من السلطة المختصة، حيث تمثل هذه العقوبة في الحبس المتراوح من سنتين إلى خمس (5) سنوات والغرامة من 200 ألف إلى 500 ألف دج[2].

وننوه إلى أن الشروع في إرتكاب أي من الجرائم المذكورة أعلاه يعاقب عليه بالعقوبات المقررة للجريمة ذاتها[3]، كما وأنه في حال ارتكاب الجريمة عن طريق شخص معنوي، توقع عليه العقوبات المنصوص عليها في قانون العقوبات[4]، والتي تبدأ من الغرامة من مرة واحدة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي، وتصل إلى غلق المؤسسة مؤقتاً أو حلّها[5].

ومما يلفت إنتباهنا من المواد 54 إلى 57 أعلاه، هو تقريرها لعقوبات مغلظة للتجاوزات التي تطال الحياة الخاصة للأفراد بالوسائط الإلكترونية، مع العلم أن المادة 301 مكرر1 من قانون العقوبات ومثلما سبق وأشرنا تقرِر عقوبات أخف لنفس التجاوزات، ما يجعلنا نتساءل: في حال وقع إعتداء على الحياة الخاصة للفرد بإحدى الوسائل الإلكترونية، وفي ضوء عمومية نص المواد 54 إلى 57 من القانون رقم 18-07 وعدم تحديدها بدقة لصفة مرتكب الجرم، هل يطبِّق القاضي هذه المواد أم يطبق المادة 301 مكرر1 من قانون العقوبات؟

إجابة على هذا التساؤل، نعتقد بأنه على الرغم من عمومية نص المواد من 54 إلى 57 أعلاه فإن القاضي سيطبق إحدى هذه المواد في حال أُرتكِب الجرم من قبل أحد المؤتمنين قانوناً على المعطيات الشخصية والمسؤولين عن معالجتها، كموظفي الهيئات المكلفة بتسجيل وحفظ المعلومات البيومترية ومزودي خدمة الأنترنت، بينما سيطبق المادة 301 مكرر1 من قانون

---

[1] . المادة 54 من القانون رقم 18-07 أعلاه.

[2] . المادة 57 من القانون رقم 18-07 أعلاه.

[3] . المادة 73 من القانون رقم 18-07 أعلاه.

[4] . الادة 70 من القانون رقم 18-07 أعلاه.

[5]. المادة 18 مكرر من قانون العقوبات الجزائري المعدل والمتمم.

العقوبات فيما لو تم اِرتكاب الجرم من قبل أحد الأفراد العاديين. ذلك أننا نرى بأن الأحكام الجزائية الواردة في القانون رقم 18-07 لا تخص الأفراد العاديين، وإنما تخص الأشخاص الطبيعية والمعنوية التي -بحكم نشاطها- تستطيع الوصول وبشكل قانوني للمعطيات الشخصية للأفراد ومعالجتها، وذلك ما لم يذكره القانون بشكل صريح. فصحيحٌ أن المادة السادسة منه إستثنت من مجال تطبيقه عمليات المعالجة التي لا تتجاوز الاستعمال الشخصي أو العائلي شرط عدم إحالتها إلى الغير أو نشرها، بما يفيد بأن عمليات المعالجة للمعطيات الشخصية الممارسة في إطار الاستعمال الشخصي والمتبوعة بالنشر غير مشمولة بالاستثناء، ومن ثم تنطبق عليها أحكام القانون رقم 18-07، إلاّ أننا ومن جهة أخرى نجد هذا القانون يمنع إطلاع الغير على المعطيات الشخصية إلاّ لدواعي إنجاز الغايات المرتبطة مباشرة بمهام المسؤول عن معالجة هذه المعطيات ومهام هذا الغير الذي يتم اِطلاعه، وبعد الموافقة المسبقة للشخص المعني[1]، كما أنه يشترط ضمن أحكامه إستيفاء إجراء التصريح لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو الحصول على ترخيص منها، لأجل نشر المعطيات الشخصية للأفراد[2]! وهو ما لا يمكن تصوّره بالنسبة لحالات النشر التي يقوم بها الأفراد العاديون.

فلو سلّمنا جدلاً بأن الالتزامات المنصوص عليها في القانون رقم 18-07 أعلاه تخص حتى عمليات النشر التي يقوم بها الأفراد العاديون عبر مواقع التواصل الاجتماعي، فذلك يعني بأنه ينبغي أن يكون للسلطة المذكورة جيش من الموظفين يعمل ليل نهار حتى يستقبل التصريحات بنشر الصور والمعطيات الخاصة بالأفراد والتي تفرضها المادة 12 من القانون المذكور، وتمنح وصولات الاستلام والتراخيص التي تتطلبها المواد 13، 17 و21 من ذات القانون، وهو ما لا يقبله المنطق. ثم إن ما يعزز اِعتقادنا هو تضمين القانون رقم 18-07 بنداً يتيح توقيع العقوبات المنصوص عليها في المادة 301 مكرر من قانون العقوبات وسالفة الذكر، على أعضاء السلطة وأمينها التنفيذي في حال إفشائهم لمعلومات محمية بموجب ذات القانون[3]، فما من سبب هنا يدعوا إلى استثناء هؤلاء الأشخاص من العقوبات المنصوص عليها في المواد من 54 إلى 57 من القانون رقم 18-07 إلاّ لكونهم من غير المسؤولين عن معالجة البيانات الشخصية.

---

[1]. المادة 7 فقرة 3 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2]. أنظر المواد 12، 13، 17 و21 من القانون رقم 18-07 أعلاه.

[3]. المادة 62 من القانون رقم 18-07 أعلاه.

وبالنتيجة، وبشأن القصور الذي يطبع المادة 301 مكرر1 وسالف الإشارة أعلاه، نعتقد بأن أحكام القانون رقم 18-07 لا تسد منه إلاّ ما تعلق بعمليات النشر التي تقوم بها الهيئات المؤتمنة على المعطيات الشخصية المتحصل عليها برضا الأفراد المعنيين بها، أما عمليات نشر الصور والمعطيات الخاصة للأفراد من قبل أفراد عاديين بغير رضا المعنيين بها فتبقى بعيدة عن العقاب، وهو ما يستدعي من المشرع مراجعة للمادة 301 مكرر1.

في المقابل، إذا ما ألقينا نظرة على موقف المشرع الإماراتي من جرائم انتهاك حرمة الحياة الخاصة بطريق الأنترنت سنجد بأنه كان أكثر وضوحاً ودقة، ذلك أنه وبموجب المادة 21 من القانون الاتحادي رقم 5 لسنة 2012 نص صراحة على تجريم الاعتداء على خصوصية الغير؛ بما يشمل إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية ويشمل نقل الصور الإلكترونية وكشفها، مقرّراً لهذه الأفعال عقوبة الحبس التي لا تقل عن ستة (6) أشهر والغرامة التي تتراوح بين 150 ألف و 500 ألف درهم إماراتي. وكنّا نود لو أن المشرع الجزائري سار على ذات النهج وجاء بنصوص خاصة تجرم الاعتداء على الحياة الخاصة بطريق الأنترنت، لاسيما وأن هذه الأخيرة أضحت الوسيلة الأكثر شيوعاً لارتكاب الجريمة المذكورة، أو على الأقل كنّا نتمنى لو أنه سد القصور الذي لا يزال يعتري المادة 301 مكرر1.

خاتمة:

من خلال تحليلنا للأحكام التجريمية والعقابية ذات الصلة بجرائم التعبير الماسة بالأفراد، نستنتج بأن المشرع الجزائري بقي رهيناً للنظرة التقليدية في تجريم بعض السلوكات ذات الصلة بالتعبير عن الرأي. لكن على الرغم من ذلك، وبالنظر لعمومية أسلوب الصياغة الذي إعتمده في كثير من المواد، لاحظنا بأن هذه المعالجة التقليدية إستطاعت -نسبياً- مواكبة التطور الحاصل في مجال الاتصال الإلكتروني. فكلما قام المشرع الجزائي بتعداد طرق علانية السلوك المجرّم على سبيل المثال، كلما تحقق إنسجام النص مع أي تطورات تقنية قد تظهر في المستقبل. وعلى العكس من ذلك، كلما قام بتعداد هذه الطرق على سبيل الحصر، كلما قلّت فرص تكيّف النص مع التطورات التقنية الحاصلة، وهذا يحيلنا إلى الشروط التي ينبغي أن تتوافر في عملية صياغة النص القانوني والتي من أهمها بعد النظر عند القائم بالصياغة.

فالنص القانوني لا يوضع من حيث المبدأ لمعالجة مسألة آنية فحسب، بل لمعالجة مسألة تهم المجتمع وتمتد في الزمن، وكل قصور في صياغته قد ينعكس بالسلب على النظام الاجتماعي، وهو ما ظهر غداة ذيوع تقنية الهاتف المتعدد الوسائط في الجزائر بداية الألفية الثالثة، والتي واكبها

عدم إحاطة النصوص التجريمية والعقابية بهذه التقنية حينها، بشكل أدى إلى ظهور العديد من التجاوزات التي أرّقت بال الأسر الجزائرية، وذيوع مظاهر الفاحشة والابتزاز وسط المجتمع، وإستمر الحال كذلك لغاية تبني القانون رقم 06-23 سالف الإشارة.

وقد لاحظنا من خلال هذه الدراسة أن بعض الأحكام التجريمية والعقابية ذات الصلة بجرائم التعبير الماسّة بحقوق الأفراد بقيت منسجمة مع التطورات التي عرفها قطاع الاتصال الإلكتروني، لاسيما ما تعلق منها بجرائم القذف والسب العلني. ولكن في المقابل، وقفنا على أن المادة 342 من قانون العقوبات تتيح معاقبة كافة أفعال التحريض على الفسق وفساد الأخلاق التي قد تطال القصّر، ولكنها لا تقرّر أي عقوبة للشخص المعنوي في حال حصل التحريض من قبل أحد ممثليه ولحسابه. كما لاحظنا بأن صياغة المادة 345 من ذات القانون تتيح متابعة أي أجنبي يقدم إلى الجزائر يكون قد نشر اِنطلاقاً من دولته مواداً إباحية تشجع على الفسق وفساد الأخلاق، بصرف النظر عما إذا كان نشاطه انطلاقاً من دولته قانوني أو لا.

وبخصوص سلوكات التعبير المنتهكة لحرمة الحياة الخاصة، لاحظنا بأن المادة 164 من قانون البريد والاتصالات الإلكترونية وهي تجرِّم فعل نشر المراسلات الإلكترونية استطاعت مواكبة التطور الحاصل في مجال الاتصال الرقمي، وسد النقص الذي اعترى المادتين 137 و303 من قانون العقوبات والمادة 127 من قانون البريد والمواصلات السلكية واللاسلكية. كما لاحظنا بأن المادة 301 من قانون العقوبات وبالنظر لعمومية نصها استطاعت الإحاطة بكافة أشكال الممارسة غير المسؤولة لحرية التعبير المفضية إلى انتهاك السر المهني.

ولكننا في المقابل وقفنا على أن أحكام المادة 303 مكرر1 من قانون العقوبات تفيد بأن أفعال نشر وإستعمال الأحاديث والصور الخاصة بغير رضا صاحبها لا يكون معاقباً عليها إذا ما تم التحصّل عليها برضاه، وهو ما من شأنه أن يجعل الكثير من أفعال تداول الصور والتسجيلات الخاصة للأفراد عبر الأنترنت بعيدة عن المتابعة جزائية. وقد لاحظنا بأن أحكام القانون رقم 07-18 لا تسد من القصور الذي طبع المادة 303 مكرر1 أعلاه إلاّ ما تعلق بعمليات النشر التي تقوم بها الهيئات المؤتمنة على المعطيات الشخصية المتحصل عليها برضا الأفراد المعنيين بها، أما عمليات نشر الصور والمعطيات الخاصة للأفراد التي تتم من أفراد عاديين بغير رضا المعنيين بها فتبقى بعيدة عن العقاب.

وعليه، ومع تثميننا للأحكام الإيجابية المتضمنة في قانون البريد والمواصلات الإلكترونية وفي القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

وكذا في قانون العقوبات، فإننا نعتقد بضرورة مراجعة هذا الأخير على النحو الذي يجعل أحكامه مواكبة للتطور الرقمي، حيث نوصي بمراجعة المادة 301 مكرر1 بما يجرِّم نشر الصور والأحاديث الخاصة بصرف النظر عن كيفية الحصول عليها، طالما كان النشر والاستعمال بغير رضا صاحبه، ومراجعة المادة 342 على النحو الذي يقر المسؤولية الجزائية للشخص المعنوي فيما لو وقع السلوك الإجرامي من قبل أحد ممثليه ولحسابه، وكذا مراجعة المادة 345 من ذات القانون بما يشترط توجيه سلوك التحريض على الفسق الإشارة إلى القصر الجزائريين في حال وقع من أشخاص أجانب وانطلاقاً من خارج أراضي الوطن. ولكن قبل ذلك، نعتقد بأنه ينبغي على الدولة الجزائرية أن تطور ما يلزم من البرامج الإلكترونية لمنع أي بث للمحتويات الماسة بالآداب العامة والأخلاق والقيم الإسلامية، وتضع أحكاماً قانونية تمنع بث مثل هذه المحتويات في الجزائر، وكذا تُفعّل أحكام المادة 12 من القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في شقها الذي يلزم مقدمي خدمات الأنترنت بالتدخل الفوري لسحب أي محتويات إلكترونية المخالفة للقوانين.

الفاتورة الالكترونية والجرائم الواقعة عليها

The electronic bill and the crimes committed against it

د. طالب محمد كريم أستاذ محاضر أ

معهد الحقوق والعلوم السياسية

المركز الجامعي مغنية - الجزائر

مقدمة:

تلعب الفاتورة دورا هاما في تحقيق شفافية الأسعار ومن أهم السندات التي تثبت المعاملات التجارية بصفة عامة والإلكترونية بصفة خاصة، وبالتالي تعمل على تعزيز الجباية حيث يتم عن طريقها متابعة حركة رؤوس الأموال.

ونظرا لازدهار التجارة الالكترونية، حيث يتم العقد بين طرفين غير حاضرين وبالتالي لا يتم منح الفاتورة بصورة مادية، حلت مكانها الفاتورة الالكترونية التي تمنح من طرف المتعامل بمجرد انعقاد العقد الالكتروني.

ولقد لاقت الفاتورة الالكترونية تحديا جديدا مرتبط أساسا بقانون الجباية الدولية، لكونها تعتمد على مبدأين أساسيين يصعب تطبيقهما على مستوى الالكتروني، وهما: مبدأ الإقليمية لارتباطها بالقانون الضريبي المتعلق أساسا بقطر الدولة، أما المبدأ الثاني فهو سلطة فرض الضريبة على كل نشاط تجاري أو مدني يتم ابرامه أو إنجازه على مستوى إقليم الدولة، لذلك توجد صعوبة في التحقق على مستوى الشبكات وصعوبة في التعقب والمراقبة من طرف إدارة الضرائب لعجزها عن تحديد مكان العون الاقتصادي، كما أن التعامل عن طريق الأنترنت يتعدى كل الحدود يصعب من خلاله تحديد مكان التعامل التجاري.

كل هذا يدفعنا للتساؤل حول الممارسات غير المشروعة التي يمكن أن تقع على الفاتورة الالكترونية؟ يعني هل هي نفسها في الفاتورة المادية العادية أم تختلف باختلاف الوسط المتعامل فيه؟

للإجابة عن هذا التساؤل لابد أن نتطرق للإطار المفاهيمي للفاتورة الالكترونية ثم إلى الجرائم الواقعة عليها.

المبحث الأول: الإطار المفاهيمي للفاتورة الالكترونية

تلعب الفاتورة دورا هاما في تحقيق المعاملات التجارية الالكترونية، وبالتالي تعمل على تعزيز وتدعيم مبدأ حرية الأسعار في سوق افتراضي تكون فيه المنافسة حرة.

ونظرا لأهمية الفاتورة بصفة عامة جعلها المشرع إجراء إلزاميا يقع على عاتق العون الاقتصادي، في نص المادة 20 من قانون رقم 18-05 المتعلق بالتجارة الالكترونية[1] التي تحيلنا إلى القواعد العامة فيما يخص الفاتورة الممنوحة في إطار التجارة الإلكترونية بنصها على: " يترتب على كل بيع لمنتوج أو تأدية خدمة من طرف الاتصالات الالكترونية، إعداد فاتورة من قبل المورد الالكتروني، تسليم للمستهلك الالكتروني.

يجب أن تعد الفاتورة طبقا للتشريع والتنظيم المعمول بهما.

يمكن أن يطلب المستهلك الالكتروني الفاتورة في شكلها الورقي"

وتنص المادة 10 من القانون 04-02 المعدلة بالقانون 10-06[2] بصفة صريحة سواء تعلق الأمر بالبيع أو بتأدية خدمة على الزامية التعامل بالفاتورة فيما بين الأعوان الاقتصاديين، وحتى

---

[1] قانون 18-05 المتعلق بالتجارة الالكترونية مؤرخ في 24 شعبان 1439 الموافق ل10 ماي 2018، عدد الجريدة الرسمية 28 المؤرخة في 30 شعبان 1439 الموافق ل 16 ماي 2018، ص.8.

[2] المادة 10 من القانون 04-02 المعدلة بموجب المادة 120 من قانون رقم 17-11مؤرخ في 08 ربيع الثاني عام 1439 الموافق ل 27 ديسمبر سنة 2017 يتضمن قانون المالية لسنة 2018 المنشور في ج.ر. عدد76 ل 09 ربيع الثاني عام 1439 الموافق ل 28 ديسمبر سنة 2017، تنص على ما يلي: " يجب أن يكون كل بيع سلع، أو تأدية خدمة لبن الأعوان الاقتصاديين الممارسين للنشاطات المذكورة في المادة 2 أعلاه، مصحوبا بفاتورة أو بوثيقة تقوم مقامها.

يلزم البائع أو مقدم الخدمة بتسليم الفاتورة أو الوثيقة التي تقوم مقامها ويلزم المشتري بطلب أي منهما، حسب الحالة، وتسلمان عند البيع أو عند تأدية الخدمة.

استثناءا مما ورد أعلاه، فيما يخص تجار التجزئة، يسمح أن يتم بيع المنتجات التبغية من قبل المصنعين أو الموزعين المعتمدين من قبل وزارة المالية، إلى تجار التجزئة، ويشار إليهم ب "المشتري النقدي" من خلال إصدار فاتورة بيع للمشتري تحت مسمى "فاتورة نقدي" وإصدار وصل صندوق يحتفظ به البائع " المصنعون أو الموزعون المعتمدون من قبل وزارة المالية، على أن يتكفل البائع بتسديد الضرائب المستحقة على تاجر التجزئة في هذه الحالة، وهي الضريبة على القيمة المضافة والضريبة على النشاط المهني.

يسود هذا النص على أي نص آخر في هذا الشأن ورد في قانون أو مرسوم أو قرار أو تعليمة.

يجب أن يكون البيع للمستهلك محل وصل صندوق أو سند يبرر هذه المعاملة، ويجب أن تسلم الفاتورة إذا طالبها الزبون".

لفائدة المستهلك إن هو طلبها صراحة، وهنا المشرع لم يذكر الفاتورة الالكترونية بوجه الخصوص بل جعلها الزامية سواء في التجارة التقليدية أو التجارة الالكترونية كما تضمنت هذه المادة في تعديلها المشار إليها أدناه عبارة " الوثيقة التي تقوم مقامها".

هناك بعض النشاطات والمهن يكون التعامل فيها من بيع أو تأدية خدمة بين الأعوان الاقتصاديين، بوثائق عرفية متداولة ومعروفة في وسطهم المهني، هذه الوثائق لا تخضع لأي تنظيم قانوني بل تنظمها الأعراف المهنية، من بين أهم النشاطات التي تتعامل بهذه الوثائق نشاط الفلاحة، تربية المواشي وبهدف حماية هذه النشاطات من المضاربة التي تؤدي إلى الارتفاع الفاحش للأسعار ومنه حماية المنتج الوطني بصفة عامة، وحماية الفلاح بصفة خاصة، تم اعتبار هذه الوثائق كفواتير، ذلك نظرا لصعوبة فرض التعامل بالفاتورة في هذا النوع من المعاملات[1]، أو قد يقصد بها الوثيقة الالكترونية تماشيا مع التجارة الالكترونية.

إن الفاتورة هي وثيقة مهمة وفعالة لتكريس الممارسات التجارية، وقد فصل فيها المشرع في عدة مواد مقسمة بين الفصل الثاني من القانون 04-02 المعنون بالفوترة، والمرسوم التنفيذي 05-468 الذي يحدد شروط تحرير الفاتورة[2]، وكذا المرسوم التنفيذي 16-66 الذي يحدد الوثيقة التي تقوم مقام الفاتورة وكذا فئات الاعوان الاقتصاديين الملزمين بالتعامل بها[3]، وحتى تماشي والغرض المنوط بها، تدخل المشرع الجزائري وعدل المادة 10 من القانون 04-02 بموجب القانون 10-06 كما سبق الذكر.

المطلب الأول: تعريف الفاتورة

هناك عدة تعريفات الفقهية والقانونية

فرع أول: التعريف القانوني

[1] الجريدة الرسمية للمناقشات، الفترة التشريعية السادسة، الجلسة العلنية المنعقدة يوم الاثنين 12 يوليو سنة 2010 ص.ص. 5،4.

[2] المرسوم 05-468 السابق ذكره.

[3] مرسوم تنفيذي رقم 16-66 مؤرخ في 07 جمادى الأولى عام 1434، الموافق ل 16 فبراير سنة 2016، يحدد نموذج الوثيقة التي تقوم مقام الفاتورة وكذا فئات الأعوان الاقتصاديين الملزمون بالتعامل بها، المنشور في الجريدة الرسمية عدد 10 المؤرخة في 13 جمادى الأولى عام 1437 الموافق ل 22 فبراير سنة 2016. ص.ص. 3-9.

وبالرجوع إلى التشريعات السارية المفعول والتي تمت بصلة مباشرة لموضوع الفاتورة، نجد أن موضوع الفاتورة يتقاسمه كل من قانون الجمارك[1] والقانون التجاري الجزائري[2]، والتشريع الجبائي، فضلا عن القانون 04-02 والمرسوم التنفيذي 05-468 وكذا المرسوم التنفيذي 16-66، إلا أننا لم نجد أي تعريف قانوني للفاتورة وهو منطقي باعتبار أن التعريف ليس من اختصاص التشريع.

في الوقت الذي خصها فيه بمرسوم تنفيذي 05-468 بــــــ 21 مادة، لم يتدارك المشرع الجزائري هذا النقص ليسعف الباحثين بتعريف قانوني.

---

[1] قانون رقم 79-09 المؤرخ في 29 شعبان عام 1399 الموافق ل 21 يوليو سنة 1979 المتضمن قانون الجمارك المعدل والمتمم. المنشور في الجريدة الرسمية عدد 30 المؤرخة في 29 شعبان عام 1399 الموافق ل 24 يوليو سنة 1979، ولقد نص على عقد تحويل الفاتورة في المواد من 543 مكرر 14 إلى المادة 543 مكرر 18 والتي جاءت فيها على ما يلي:

المادة 543 مكرر14 " عقد تحويل الفاتورة هو عقد يحل بمقتضاه شركة متخصصة تسمى وسيط محل زبونها المسمى المنتمي، عندما تسدد فورا لهذا الأخير المبلغ التام لفاتورة لأجل محدد ناتج عن عقد، وتتكفل بتبعية عدم التسديد وذلك مقابل أجر"

المادة 543 مكرر 15' يجب أن يبلغ المدين فورا بنقل حقوق الديون التجارية إلى الوسيط بواسطة رسالة وصى عليها بوصل الاستلام"

المادة 543 مكرر 16" يترتب على تحويل الديون التجارية، نقل كل الضمانات التي كانت تضمن تنفيذ الالتزامات لفائدة الوسيط"

المادة 543 مكرر 17 " ينظم الوسيط المنتمي بكل حرية وعن طريق الاتفاق، كل الكيفيات العملية لتحويل الدفعات المطابقة لحواصل التنازل"

المادة 543 مكرر 18" يحدد محتوى إصدار الفاتورات لأجل محدد وشروطه وكذا شروط تأهيل الشركات التي تمارس تحويل الفاتورات عن طريق التنظيم".

[2] الأمر رقم 75-59 مؤرخ في 20 رمضان عام 1395 الموافق ل 26 سبتمبر سنة 1975 يتضمن القانون التجاري المعدل والمتمم. المنشور في الجريدة الرسمية عدد78 المؤرخة في 24 رمضان عام 1395 الموافق ل 30 سبتمبر سنة 1975. حيث تنص المادة 226 على أن يشترط تقديم فواتير الشراء أو سندات التسليم أو أية وثيقة أخرى لإثبات حيازة البضائع بصفة مشروعة، حيث

يشترط قانون الجمارك تبريرها بمستندات عبر كامل الإقليم الجمركي، وفي قرارها رقم 2878333 المؤرخ في 2004/04/06 المنشور في المجلة القضائية عدد 02 لسنة 2006 ص. 481، اعتبرت المحكمة العليا عدم الفوترة جريمة تندرج ضمن جرائم التهريب في حالة حيازة البضاعة.

وفي قراءة لهذا المرسوم الذي جاء تطبيقا لأحكام المادة 12 من القانون 04-02 التي تنص على أنه يجب أن تحرر الفاتورة ووصل التسليم والفاتورة الإجمالية وكذا سند التحويل وفق الشروط والكيفيات التي تحدد عن طريق التنظيم، وبناء على ذلك تم إعداد المرسوم التنفيذي 05-468 المؤرخ في 10 ديسمبر سنة 2005 المحدد لشروط تحرير الفاتورة، سن التحويل، وصل التسليم، والفاتورة الاجمالية.

وتتلخص الأهداف الرئيسية المحددة في هذا الإطار التنظيمي في ما يلي:

- تكريس نزاهة وشفافية العمليات التجارية والممارسة من طرف الأعوان الاقتصاديين اتجاه المستهلكين والإدارات التجارية والضريبية كما سبق القول أعلاه.
- تحديد بصفة دقيقة وبسيطة أهم البيانات الضرورية اللازم إدراجها في الوثائق المذكورة آنفا، وهذا استجابة للمتطلبات المتعلقة بضمان نزاهة العمليات التجارية وسيولة قواعد السوق[1].
- توحيد قواعد واجراءات إنشاء هذه الوثائق الجديدة استجابة لمتطلبات السوق.

واستثناءا لهذه الأهداف فإن النص يقترح:

- التعريف لبعض المفاهيم ذات الطابع التجاري والمالي والتقني (اقتطاعات، تخفيضات، انتقصات، نقل الكتروني...)[2]، في الوقت الذي أغفل التعريف بالفاتورة، وسند التحويل ووصل التسليم والفاتورة الاجمالية، والتي تعد جميعها أولى بالتعريف والتحديد القانوني، واكتفى بتحديد البيانات الضرورية الواجب احتوائها فيها.
- إحصاء البيانات الإضافية التي يجب إبداءها على الفاتورة عند الاقتضاء والمتعلقة لا سيما بالتخفيضات التجارية (تخفيضات، انتقصات، اقتطاعات)[3].
- مصاريف النقل، فوائد القروض، بالإضافة إلى الوساطة وإيداع الرسم[4].

---

[1] علاوي زهرة، الفاتورة وسيلة شفافية للممارسات التجارية، مذكرة ماجستير في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة وهران، السنة الجامعية 2013/2012، ص.9.

[2] المادة 04 و 06 من المرسوم التنفيذي 05-468 السابق ذكره.

[3] المادة 05 من المرسوم التنفيذي 05-468 السابق ذكره.

[4] المادة 07 من المرسوم التنفيذي 05-468 السابق ذكره.

- تحديد الحالات والشروط التي يتم الترخيص من خلالها باستعمال وصل التسليم، سند التسليم والفاتورة الاجمالية[1].
- تكريس مبدأ الفاتورة عن طريق النقل الالكتروني، وهذا بغرض الاستجابة لمقتضيات عصرنة أدوات التسليم وانفتاح الاقتصاد الوطني على التكنولوجيا الحديثة للإعلام[2].

فرع ثاني: التعريف الفقهي:

توجد عدة تعريفات فقهية وهي كالآتي:

" بأنها كتابة تنشأ بمناسبة بيع أو أداء خدمات التي تثبت وجود هذه العملية التجارية وتوضح شروطها"[3].

كما تعرف كذلك: "وثيقة مكتوبة، حسابية تحرر وقت انعقاد البيع، أو عند تقديم الخدمة لإثبات وجود هذا العقد، متضمنة شروط انعقاده وشروط تنفيذه"[4].

كما تم تعريفها بأنها: " وثيقة حسابية يدون فيها بيان البضائع المبيعة أو الأعمال المنجزة ومفصل ثمن كل قيد من قيودها إلى جانبه، وتقوم الفاتورة في الأمور التجارية دليلا على العقد، أما الفاتورة المشار إليها بالإلغاء أو التسديد فإنها تبرئ ذمة المدين"[5].

أما الفاتورة الالكترونية وإن كان ينطبق عليها كل التعاريف السابقة لكن هناك تعريف خاص بها وهو: "الفاتورة الالكترونية هي نظام منخفض التكاليف لمعالجة المعاملات التي تستفيد من تكنولوجيا المعلومات لتحويل عملية إعداد الفواتير اليدوية والورقية إلى صيغة الكترونية أكثر فاعلية في معالجة رسائل البيانات والمحافظة على السجلات"[6]. عُرِّفت الفاتورة الالكترونية في المبدأ التوجيهي رقم (2001/115/EC) الصادر عن المجلس الأوروبي بأنها: "إرسال الفواتير

---

[1] المادة 14 وما يليها من المرسوم التنفيذي 05-468 السابق ذكره.

[2] المادة 11 من المرسوم التنفيذي 05-468 السابق ذكره.

[3] أشارت إليه علاوي الزهرة، مرجع سابق، ص.7.

[4] أشارت إليه لطاش نجية، لطاش نجية، مبدا الشفافية في قانون المنافسة في الجزائر، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر 01 يوسف بن خدة، السنة الجامعية: 2003/2004، ص.44.

[5] أشار إليه طالب محمد كريم، تقييد المنافسة عن طريق الأسعار، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، سنة 2020، ص.147.

[6] تم الإشارة إليها في الموقع https://www.dbresearch.com/prod/rps_en/hidden_global_search.aliasالإطلاع في 2020/06/05 على الساعة 17سا49

عبر الوسائل الالكترونية؛ أي نقلها إلى المتلقي باستخدام معدات الكترونية لمعالجة وتخزين البيانات". مع انطلاق الفاتورة الالكترونية، استبدلت فاتورة الورقة التقليدية بنسخة الكترونية مما أزال كثيراً من سلبياتها بينما حافظ على الفاتورة بمثابة وثيقة قائمة.

المطلب الثاني: أطراف الفاتورة الإلكترونية

لتحديد مدى إلزامية تقديم الفاتورة، يجب علينا الإحاطة بهذا النطاق من حيث النطاق الشخصي، مفرقين بين نوعين من العلاقة، علاقة الأعوان الاقتصاديين فيما بينهم، والعلاقة بين العون الاقتصادي والمستهلك، أي هو العون الاقتصادي هو ملزم بتسليم الفاتورة إلا في علاقته مع عون اقتصادي آخر أو حتى في علاقته مه المستهلك؟

كذلك يجب علينا التطرق إلى النطاق الموضوعي للفاتورة من حيث محل الفاتورة وأخيرا النطاق الزماني، أي متى يلتزم العون الاقتصادي بتحرير الفاتورة وماهي المدة القانونية التي يجب عليه المحافظة عليها؟

فرع أول: علاقة المتعاملين الاقتصاديين فيما بينهم

إن المادة 10 من القانون 04-02 والمادة 23 المرسوم التنفيذي رقم 05-468 المحدد لشروط تحرير الفاتورة وسند التحويل ووصل التسليم والفاتورة الاجمالية وكيفيات ذلك السابق ذكره،.

نصت المادة 10 من القانون 04-02 المعدل والمتمم على أنه: " يجب أن يكون كبيع سلع، أو تأدية خدمات بين الأعوان الاقتصاديين الممارسين للنشاطات المذكورة في المادة 02 أعلاه مصحوبا بفاتورة أو بوثيقة تقوم مقامها.

يلزم البائع أو مقدم الخدمة بتسليم الفاتورة أو الوثيقة التي تقوم مقامها ويلزم المشتري بطلب أي منهما، حسب الحالة، وتسلمان عند البيع أو عند تأدية الخدمة".

يلاحظ من المادة أن المشرع أوجب أن يكون كل تعامل بين الأعوان الاقتصاديين مصحوبا بفاتورة أو وثيقة تقوم مقامها، تفرغ في محرر مكتوب، والكتابة هنا يمكن أن تكون مادية او إلكترونية يتكون من أصل وصورة أو عدة صور، وحدد لها البيانات التي يجب أن تحتوي عليها[1].

---

[1] المادة 02 من المرسوم التنفيذي 05-468 السابق ذكره.

ويمكن أن تحل محل الفاتورة الالكترونية بدائل حددها القانون[1]، ويجب على العون الاقتصادي تسليمها للمشتري المهني، كما يجب على هذا الأخير أن يطلبها من البائع، فالمشتري مسؤول مثل البائع على طلب الفاتورة الالكترونية، ومسؤول أيضا على هما ورد فيها وبمراقبتها[2]، ويجب أن تسلم بمجرد إجراء البيع أو تأدية الخدمة[3].

أولا: البيانات العامة الواجب توافرها في الفاتورة الالكترونية :

يمكن تقسيم البيانات التي أوردها المشرع الجزائري في المادة 3 من المرسوم التنفيذي رقم 05-468 إلى ثلاثة أنواع: بيانات خاصة بالأطراف، بيانات متعلقة بالسعر، وأخرى متعلقة بالفاتورة نفسها.

1- بيانات خاصة بالأطراف:

تنص المادة 12 من القانون 04-02على أنه: " يجب أن تحرر الفاتورة ووصل التسليم والفاتورة الاجمالية وكذا سند التحويل وفق الشروط والكيفيات التي تحدد عن طريق التنظيم".

وبالتالي أحال المشرع الشروط الشكلية للفاتورة إلى التنظيم والذي هو المرسوم التنفيذي رقم 05-468 السالف ذكره، حيث تنص المادة 03 منه على البيانات المتعلقة بأطراف الفاتورة وفرق العون الاقتصادي الذي قد يكون بائعا أو مشتريا.

يجب أن تذكر بيانات العون الاقتصادي في الفاتورة سواء كان بائعا أو مشتري، كما يلي[4]:

- اسم الشخص الطبيعي ولقبه.
- تسمية الشخص المعنوي أو عنوانه التجاري.
- العنوان ورقم الهاتف والفاكس وكذا العنوان الالكتروني عند الاقتضاء.
- الشكل القانوني للعون الاقتصادي وطبيعة نشاطه.

---

[1] المرسوم التنفيذي 16-66 الذي يحدد نموذج الوثيقة التي تقوم مقام الفاتورة وكذا فئات الأعوان الاقتصاديين الملزمون بالتعامل بها. السابق ذكره.

[2] المحكما العليا، غرفة الجنح والمخالفات، قرار رقم 267580 مؤرخ في 2004/07/07، المجلة القضائية، العدد 02، 2004. أنظر محمد الشريف كتو، قانون المنافسة الممارسات التجارية، المرجع السابق، ص.89.

[3] المادة 02 من المرسوم التنفيذي 05-468 السابق ذكره.

[4] المادة 03 من المرسوم التنفيذي 05-468 السابق ذكره.

- رقم السجل التجاري.
- رقم التعريف الإحصائي.
- رأسمال الشركة، لا يشترط إذا كان العون الاقتصادي مشتريا، يذكر فقط إذا كان العون الاقتصادي بائعا.

هذه البيانات المتعلقة بالعون الاقتصادي اجبارية، بحيث استعمل المشرع مصطلح "يجب" وهذا يدل على أن القاعدة آمرة أي الإلتزام اجباري، كما أن البينات جاءت على سبيل الحصل لا المثال، إذ تكمن أهمين الطابع الالزامي لهذه البيانات، في التحديد الدقيق والوافي للفاتورة النافي للجهالة والشك، وحتى يكون للفاتورة حجة على محررها.

2- بيانات متعلقة بالسعر وطرق الدفع:

يجب أن تتضمن الفاتورة الالكترونية سعر السلعة أو الخدمة المحدد أثناء انعقاد العقد، ويجب تحديد السعر الصافي قبل حساب التخفيضات وقبل إضافة الرسوم.

والفائدة من كتابة السعر دون التخفيضات والرسوم، هي لتعرف المشتري أن ليس موضوع عمل تمييزي، وكذا مراقبة أي محالة للبيع بالخسارة، وبالتالي ضمان شفافية المعاملات التجارية[1].

إضافة إلى سعر المنتوج أو الخدمة يجب أن تحتوي الفاتورة الالكترونية على كافة الرسوم ومنها رسم على القيمة المضافة T.V.A ما لم يكن المشتري معفى منها بموجب القانون الجبائي.

إضافة إلى هذه البيانات المتعلقة بالسعر اضاف المشرع بيانات أخرى متعلقة بتكاليف النقل[2]، إن لم تكن مفوترة كل على حدى ولن تدخل في تكوين سعر الوحدة، إضافة إلى كل زيادة في السعر، كالفوائد المستحقة عند البيع بآجال والتكاليف التي تشكل عبء استغلال للبائع كأجور الوسطاء والعمولات والسمسرة وأقساط التأمين، عندما يدفعهما البائع وتكون مفوترة على حساب المشتري[3].

يجب أن يذكر كذلك في الفاتورة كيفيات الدفع وتاريخ تسديد الفاتورة[4].

---

1 لطاش نجية، المرجع السابق، ص.65.

2 المادة 07 من المرسوم التنفيذي 05-486 السابق ذكره.

3 المادتين 07 و08 من المرسوم التنفيذي 05-486 السابق ذكره.

4 محمد الشريف كتو، قانون المنافسة الممارسات التجارية، المرجع السابق، ص.89.

3- البيانات المتعلقة بالفاتورة بحد ذاتها:

يجب أولا أن تتضمن الفاتورة تاريخ تحريرها ورقم تسلسلها في دفتر الفواتير، ولتحديد تاريخ الفاتورة أهمية بالغة تتمثل في:

- تاريخ التحرير يعبر عن تاريخ انعقاد العقد الذي له أهمية من حيث الاثبات، من حيث بداية حساب مواعيد الدفع، التقادم...
- تاريخ الفاتورة يساعد في مكافحة الغش في تحرير الفواتير، وذلك بالرجوع إلى دفتر الفواتير.

نلاحظ أن المشرع لم يشترط تحديد تاريخ البيع أو أداء الخدمة على الفاتورة، وهذا عكس المشرع الفرنسي الذي اشترط ذلك.

أوجب المشرع كذلك الختم الندي وعلى توقيع البائع، إلا إذا حررت عن طريق النقل الالكتروني، والتوقيع هو شرط أساسي جوهري لأنه هو أساس نسبة الكتابة إلى الموقع، ذلك أن التوقيع يتضمن قبول ما هو مكتوب بالورقة، لكن حسب رأينا كان على المشرع أن يلزم حتى المشتري بالتوقيع لأنه حتى هو مسؤول عنما كتب عليها حسب قرار المحكمة العليا رقم 267580 المذكور أعلاه، وبالتالي من الأجدر حتى هو يؤشر على مضمونها.

ولكن فيما يخص الفاتورة الالكترونية فالتوقيع يكون الكتروني الذي اعترف به المشرع الجزائري في نص المادة 327 فقرة 2 من القانون المدني[1] التي تحيلنا إلى نص المادة 323 مكرر 1 من نفس القانون: " يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق...".

ثانيا: الشروط الخاصة بالفاتورة الإلكترونية:

يشترط في الفاتورة الالكترونية جملة من الشروط الخاصة حتى تكون مقبولة في الإثبات:

1- القيود الشكلية:

تتمثل أساسا في التصريح المسبق أمام إدارة الضرائب باستعمال المعلوماتية (التجارة الالكترونية) في إنشاء وإرسال الفواتير وحفظ الالكترونية، مع ضرورة التقيد بكتابة كل البيانات الضرورية في الفاتورة التقليدية.

---

[1] المادة 327 فقرة 2 من القانون المدني: " ويعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 232 مكرر 1 أعلاه"

2- شرط استرداد الفاتورة الالكترونية:

ومعنى ذلك قراءة الفاتورة عند طلبها عن طريق الحاسوب بالطريقة التي أنشأت وحفظت بها، والقراءة على شاشة الحاسوب أو عند طبعها من جديد على السند الورقي.

3- حفظ وتخزين الفاتورة في شكلها المرسل مع إمكانية طبعها في الشكل الورقي:

يقصد بذلك وضع سجل الكتروني للفواتير أو نظام خاص بمعالجة الفواتير، ويحتوي هذا السجل بأرقام وتواريخ الفاتورة ومضمونها.[1]

فرع ثاني: تسليم وصل الصندوق أو الفاتورة للمستهلك

نصت الفقرة الثالثة من المادة 10 من القانون 04-02 على أنه: " يجب أن يكون بيع السلع أو تأدية الخدمة للمستهلك محل وصل الصندوق أو سند يبرر هذه المعاملة، غير أن الفاتورة أو الوثيقة التي تقوم مقامها يجب أن تسلم إذا طلبها الزبون".

والمستهلك حسب قانون حماية المستهلك " هو كل شخص طبيعي أو معنوي يقتني، بمقابل أو مجانا سلعة أو خدمة موجهة للاستعمال النهائي من أجل تلبية حاجاته الشخصية أو تلبية حاجة شخص آخر أو حيوان متكفل به"[2].

وتوفر الفاتورة الالكترونية أو ما يقوم مقامها للمستهلك إعلام ما بعد التعاقد، يسمح له بإثبات حقوقه تجاه البائع أو مقدم الخدمة، لا سيما، فيما يتعلق بالحق في ضمان السلعة وأداء الخدمة[3].

مبحث ثاني: الجرائم المتعلقة بالفوترة الالكترونية

نلاحظ أن المشرع الجزائري عند تنظيمه للفاتورة الالكترونية اعتمد أسلوب الجزاء ليضمن احترام تلك القواعد القانونية، مما يكرس فعالة الفاتورة في تحقيق شفافية الممارسات التجارية كآلية لمكافحة جرائم الممارسات التجارية، وهناك نوعين من المخالفات وهما جريمة عدم الفوترة وجريمة الفوترة غير المطابقة، كما استحدث فعل الفواتير المزورة أو الفواتير المجاملة[4].

---

[1] قارة مولود، النظام القانوني للفوترة الالكترونية، مجلة المعارف، السنة الحادية عشر، العدد 21، ديسمبر2016، ص.ص.90-92.

[2] المادة 03 فقرة 1 من قانون 09-03 المتعلق بحماية المستهلك وقمع الغش، السابق ذكره.

[3] محمد الشريف كتو، قانون المنافسة والممارسات التجارية، المرجع نفسه، ص.91.

[4] لعور بدرة، آليات مكافحة جرائم الممارسات التجارية في التشريع الجزائري، رسالة دكتوراه في قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، السنة الجامعية 2013/2014، ص.180.

مطلب أول: الجرائم المتعلقة بوجود الفاتورة الالكترونية

وهنا نفرق بين جريمة عدم الفوترة الالكترونية وجريمة جريمة عدم مطابقة الفاتورة الالكترونية للقوانين والأنظمة.

فرع أول: جريمة عدم الفوترة الالكترونية

في البداية لا بد من الإشارة أن المشرع الجزائري لا يفرق بين المشتري والبائع في مجال الإخلال بالإلتزام، بعبارة أخرى فإن تقديم الفاتورة متى طلبت من أعوان المراقبة واجبة من كليهما، وكذلك لم يفرق بين الفاتورة المادية والالكترونية موضوع الدراسة.

لقد نصت المادة 33 ممن القانون 04-02 على ما يلي: " دون المساس بالعقوبات المنصوص عليها في التشريع الجبائي، تعتبر عدم الفوترة مخالفة لأحكام المواد 10 و11 و13 من هذا القانون، ويعاقب عليها بغرامة بنسبة 80% من المبلغ الذي كان يجب فوترته مهما بلغت قيمته".

من خلال استقراء المادة نلاحظ أن عدم الفوترة الالكترونية جريمة كلما وقعت أفعال مخالفة لمضمون المواد 10، 11، 13 من القانون 04-02، وبالتالي فصورة هذه الجريمة هي كالآتي:

أ- عقد بيع سلعة أو عقد أداء خدمات بين الأعوان الاقتصاديين (الممارسين للنشاطات الواردة في المادة 02 من القانون 04-02) الذي يتم بدون فاتورة أو وصل استلام أو فاتورة اجمالية.

ب- امتناع العون الاقتصادي عن تقديم الفاتورة الالكترونية رغم طلبها من المستهلك في عقد البيع الالكتروني أو عقد أداء الخدمات أو عدم تقديمها للموظفين المؤهلين عند أول طلب في الآجال المحددة من الإدارة المعنية[1].

ج- عدم حيازة العون الاقتصادي على سند التحويل الخاص بالسلع التي لا تكون محل معاملات تجارية والتي ينقلها إلى وحداته (للتخزين أو التحويل أو التعبئة أو التسويق)، أو عدم تقديمه للأعوان المؤهلين عند طلبه.

د- عدم تحرير أو تسليم وصل للتسليم في المعاملات التجارية الالكترونية المتكررة والمنتظمة عند بيع منتوجات لنفس الزبون أو عدم تقديمه للأعوان المؤهلين عند طلبه.

---

[1] لعور بدرة، آليات مكافحة جرائم الممارسات التجارية في التشريع الجزائري، المرجع السابق، ص.181.

ه- عدم حيازة أو تحرير أو تسليم الفاتورة الإجمالية أو عدم تقديمها للأعوان المؤهلين عند طلبها[1].

إذا وقعت صورة من هذه الممارسات تشكل الركن المادي لجريمة عدم الفوترة الالكترونية ويكفي وقوع صورة واحدة لقيام الجنحة، حيث أن كل حالة مستقلة بذاتها عن الصور الأخرى[2].

حيث يعاقب على كل هذه الصور لجريمة عدم الفوترة ب 80 % من المبلغ الذي كان يجب فوترته ومهما بلغت قيمته، وهنا تضارب في الآراء الفقهية حول مدى فعالية هذه العقوبة، حيث هناك من يراها مبالغة فيها، أين يمكنها ان تؤدي إلى إفلاس العون الاقتصادي، وهناك من يؤيدها لأن لها آثار وخيمة على الاقتصاد الوطني من خلال تهريب رؤوس الأموال إلى الخارج والتهرب الضريبي، ونحن نرى أن المشرع قد شدد كثيرا من العقوبة حيث أن هناك عقوبات جبائية تضاف على هذه العقوبة، فالأصل أن هذه العقوبة هي الحفاظ على شفافية الممارسات التجارية وليس القضاء عليها كليا.

فرع ثاني: جريمة عدم مطابقة الفاتورة الالكترونية للقوانين والأنظمة:

نكون أمام جريمة الفوترة الالكترونية غير المطابقة بمجرد تخلف البيانات الإلزامية المنصوص عليها في المرسوم التنفيذي رقم 05-468 المحدد لشروط تحرير الفاتورة السابق ذكره، حيث جاء في المادة 34 من قانون 04-02 على ما يلي: " تعتبر فاتورة غير مطابقة، كل مخالفة لأحكام المادة 12 من هذا القانون، ويعاقب عليها بغرامة من عشرة آلاف دينار (10.000 د.ج) إلى خمسين ألف دينار (50.000 د.ج.)، بشرط أن لا تمس عدم المطابقة الاسم أو العنوان الاجتماعي للبائع أو المشتري، وكذا رقم تعريفه الجبائي والعنوان والكمية والاسم الدقيق وسعر الوحدة من غير الرسوم للمنتجات المبيعة أو الخدمات المقدمة حيث يعتبر عدم ذكرها في الفاتورة عدم فوترة ويعاقب عليها طبقا لأحكام المادة 33 أعلاه".

---

[1] لعور بدرة، آليات مكافحة جرائم الممارسات التجارية في التشريع الجزائري، نفس المرجع، ص.181

[2] اعتبرت المحكمة العليا في اجتهادها بتاريخ 2004/04/06 تحت رقم 287833 أن عدم الفوترة جريمة من جرائم التهريب في حالة حيازة البضاعة، حيث يشترط قانون الجمارك تبريرها عبر كامل الإقليم الجمركي، كما قضت نفس المحكمة في قرارها رقم 260414 المؤرخ في 2001/06/25 ببراءة المتهم الذي أثبت شرعية حيازته للبضائع المستوردة بموجب فاتورة شرعية وصحيحة. قرار غير منشور أشارت إليه : لعور بدرة، آليات مكافحة جرائم الممارسات التجارية في التشريع الجزائري، نفس المرجع، ص.181

إضافة إلى العقوبات الأصلية، يمكن للقاضي أن يحكم بعقوبات تكميلية والمتمثلة في مصادرة السلع محل المخالفة، وكذا نشر الحكم أو ملخص من الحكم على عاتق العون الاقتصادي المخالف لأحكام المتعلقة بالفوترة، كما يمكن وفي حالة العود بالحكم بمضاعفة العقوبة وكذا المنع من ممارسة النشاطات التجارية لمدة مؤقتة لا يمكن أن تزيد عن 10 سنوات[1].

مطلب ثاني: جنح أخرى متعلقة بالالتزام بالفوترة الالكترونية

حرص المشرع الجزائري على تغطية موضوع الفاتورة بما يكفل الحماية الجنائية المتكاملة، حيث صدر القرار المؤرخ في 2013/08/01 المحدد لمفهوم فعل إعداد الفواتير المزورة أو فواتير المجاملة وكذا كيفيات تطبيق العقوبات المقررة عليها[2]. وهو القرار الذي جاء تطبيقا لأحكام المادة 65 من قانون المالية لسنة 2003[3]،وكذا المادة 219 مكرر[4] من قانون الضراب المباشرة والرسوم المماثلة. وبالتالي فهذه الجنح هي كالآتي:

---

[1]المواد 44 وما يليها من قانون 04-02 السابق ذكره.

[2] قرار مؤرخ في 23 رمضان عام 1434 الموافق ل 1 غشت سنة 2013، يحدد مفهوم فعل إعداد الفواتير المزورة والفواتير المجاملة وكذا كيفيات تطبيق العقوبات المقررة عليها، المنشور غي الجريدة الرسمية عدد 30 ل 21 رجب عام 1434 الموافق ل 21 ماي سنة 2014 ص.ص. 9، 10.

[3] تنص المادة 65 من قانون المالية رقم 02-11 لسنة 2003 المؤرخ في 20 شوال عام 1423 الموافق ل 24 ديسمبر سنة 2002 الجريدة الرسمية عدد 86 ل21 شوال عام 1423 الموافق ل 25 ديسمبر سنة 2002، " دون الإخلال بالعقوبات المنصوص عليها من جهة أخرى، يؤدي عدم الفوترة أو عدم تقديمها، إلى تطبيق غرامة تحدد مبالغها كما يأتي:

50000 دج بالنسبة لتجار التجزئة،

500000 دج بالنسبة لتجار التجزئة،

1000000 دج بالنسبة للمنتجين والمستوردين،

في حالة العود يتم تطبيق ضعف هذه المبالغ تصادر البضاعة المنقولة بدون فاترة وكذا وسيلة نقلها إذا كانت ملك لصاحب البضاعة.

يمكن أيضا لأعوان إدارة الضرائب المؤهلين قانونا، والذي لهم على الأقل رتبة مفتش، معاينة عدم الفوترة.

تحدد كيفيات تطبيق هذه المادة عن طريق التنظيم".

[4] تنص المادة 219 مكرر من قانون الضرائب المباشرة والرسوم المماثلة: " لا يمنح التخفيضات المشار إليها في المادة 219 أعلاه إلا بالنسبة لرقم الأعمال غير المحقق نقدا.

وبغض النظر عن كل الأحكام المخالفة يترتب على إعداد الفواتير المزورة أو فواتير المجاملة إعادة تسديد مبالغ الرسم المستحقة الدفع والتي توافق التخفيض الممنوح.

فرع اول: الفاتورة الالكترونية المزورة:

هي الفاتورة الالكترونية التي تم إعدادها دون الشروع في أي عملية تسليم أو أداء خدمة، بغرض القيام بما يأتي:

- تخفيض قواعد فرض الضريبة بالنسبة لمختلف الضرائب والرسوم.
- إخفاء عمليات الالكترونية.
- نقل تبييض رؤوس أموال.
- اختلاس أموال من الأصول وتمويل عمليات غير قانونية أو قانونية.

الاستفادة من بعض الامتيازات كالحق في الحسم في مجال الرسم على القيمة المضافة والحصول على قروض لدى المؤسسات المصرفية بغية تمويل المشارع الاستثمارية[1].

فرع ثاني: فاتورة المجاملة:

هي الفاتورة الالكترونية التي يتم من خلالها إما التلاعب أو اخفاء على الفاتورة لهوية وعنوان الممونين أو الزبائن، أو القبول الطوعي باستعمال هوية مزورة أو اسم مستعار، وذلك بهدف خفض مبلغ الضرائب الواجب دفعها، وكذا اختلاس أموال مؤسسة أو أموال شخص ما واستعمالها لأغراض مختلفة.

تمثل فاتورة المجاملة عملية شراء أو بيع أو أداء خدمة حقيقية[2].

وقد نصت المادة 37 من القانون 04-02 على عقوبة إصدار فواتير وهمية أو مزيفة بغرامة من 300000 دج إلى 10000000 دج ودون الإخلال بالعقوبات الجبائية[3].

الخاتمة:

في الأخير نلاحظ أن المشرع لم يهتم بالفاتورة الالكترونية بصفة خاصة وهذا بالرغم من صدور القانون الخاص بالتجارة الالكترونية رقم 18-05 الذي يحدد القواعد المطبقة على التجارة في العالم الافتراضي، ولما كانت الفاتورة من الوسائل الضرورية لتحقيق شفافية الأعمال التجارية بصفة عامة، ولخصوصية الفاتورة الالكترونية، نظرا لسهولة تعديلها إلكترونياعن طريق

يحدد تعريف إجراء إعداد الفواتير المزورة وفواتير المجاملة وكذا كيفيات تطبيق العقوبات المقررة عليها بموجب قررا من الوزير المكلف بالمالية".

[1] المادة 2 من القرار المؤرخ في 2013/08/01، السابق ذكره.

[2] المادة 3 من القرار المؤرخ في 2013/08/01، السابق ذكره.

[3] المواد 3 و4 من القرار المؤرخ في 2013/08/01، السابق ذكره.

قرصنة الحسابات، كذلك صعوبة تتبع حركتها وبالتالي صعوبة التحصيل الجبائي عليها أو الازدواج الضريبي في حالة صدورها خارج إقليم الدولة، لا بد على المشرع مواكبة تطور التجارة الالكترونية وحماية الاقتصاد الوطني عن طريق التأطير القانوني للفاتورة الالكترونية بصفة خاصة من خلال إفرادها بأحكام قانونية خاصة تضاف إلى أحكام المطبقة على الفاتورة التقليدية وهذا لخصوصيتها غير المادية، وصعوبة توطينها ومراقبتها من طرف إدارة الضرائب.

كذلك لابد على المشرع وضع برنامج معلوماتي أو تطبيق إلكتروني من أجل تتبع إصدار الفاتورة الالكترونية من خلال وضع أرضية يتم من خلالها منح الفاتورة الالكترونية أو إسلامها من أجل ضبط حركة رؤوس الأموال وكذا التحصيل الحسن للضريبة على القيمة المضافة، وتتبع كل الممارسات المخالفة للفوترة الإلكترونية.

ولتفادي كل تلك النقائص المذكورة قدمت منظمة التعاون والتنمية الاقتصادية خمسة حلول تكون ركيزة لأي نظام ضريبي وفوترة إلكترونية على مستوى التجارة الالكترونية وهي: الفعالية، الثقة، البساطة، الشفافية والمرونة، فإذا كرست هذه المبادئ فإن الفاتورة تحكمها نفس القواعد والمبادئ القانونية التقليدية، ومن ثم تكون الفاتورة الالكترونية بذات الفعالية التي تتمتع بها مثيلتها التقليدية، علما أن بعد التطبيقات لا تثير مشاكل في اقتطاع الضريبة مثل الضريبة المقتطعة من عمليات الإشهار التجاري على مواقع الأنترنت، خاصة وسائط التواصل الاجتماعي[1].

---

[1]أشار إليه قارة مولود، المرجع السابق، ص.29

التقليد المعلوماتي للعلامة التجارية

Forgery of the mark in the electronic

د. سالمي نضال أستاذة محاضرة "أ"

جامعة وهران 2

مقدمة :

نظرا للدور الكبير الذي تلعبه العلامة التجارية في مجال المنافسة الشريفة، والحرص على رواج البضائع واستقطاب المستهلكين، أصبح سن القوانين الخاصة بتنظيمها فرضا محتوما على كافة التشريعات وذلك لضمان التقدم و الازدهار الاقتصاديين على الصعيدين الصناعي والتجاري .

ونتيجة لأهمية العلامة التجارية على الصعيدين الدولي والمحلي والمتمثلة في تحقيق غايات كل من المنتج والمستهلك على حد السواء[1]، فإنه قد أصبح لديها العديد من الوظائف، إذ أنها أصبحت مصدرا للتمييز بين مختلف البضائع والسلع والخدمات المتعددة .

كما يضيف لها الفقه المعاصر وظيفة إعلامية وإعلانية هامة، فعن طريقها يتمكن مالكها من الإعلان عن بضاعته وتعريف المستهلكين بها، بالإضافة إلى اعتبارها أداة هامة لتوفير الحماية للمستهلكين من الغش والاحتيال الذي قد يلجأ إليهما أصحاب السلع والمنتجات أو الخدمات المقلدة والمغشوشة.[2]

ونتيجة لهذه الوظائف الهامة والمتعددة ، فقد أصبح تقليد العلامة التجارية من الجرائم المستفحلة داخل الأوساط التجارية ذلك أن هذه الجريمة قد حظيت نتيجة للثورة المعلوماتية أو الثورة الرقمية بتطور هائل حيث أصبح بالإمكان إلحاقها في دائرة الجرائم المعلوماتية لأن العلامة التجارية قد أصبحت تتعرض هي الأخرى للتقليد ، ومن ثمة يمكن حصر الإشكالية في السؤال الرئيسي التالي: ما مدى فعالية الحماية القانونية في حماية العلامات التجارية من الاعتداءات الواقعة عليها عبر شبكة الإنترنت ؟

1- حسين فتحي ،حدود مشروعية الإعلانات التجارية لحماية المتجر والمستهلك ،دار النهضة العربية ، القاهرة، 1991،ص9.

2- حمادي زوبير ، الحماية القانونية للعلامة التجارية ،الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت ، 2012،ص19. [2]

ونتفرع من هذا الإشكال الرئيسي عدة أسئلة ثانوية نحصرها في التساؤلات التالية : ماهي الطبيعة القانونية للعلامة التجارية الإلكترونية ؟و ماهو التكييف القانوني للتقليد المعلوماتي الذي يكون محله العلامة التجارية؟ وما هي نقاط اختلافه مع جريمة التقليد الكلاسيكية ؟

للإجابة على تلك الإشكاليات تم إتباع خطة بحث مقسمة إلى مبحثين تعرضنا في المبحث الأول إلى ماهية العلامة التجارية وقد سلطنا الضوء فيه على مختلف التعريفات التي أسندت لها، وكيفية تسجيلها ، ثم تعرضنا في المبحث الثاني لطرق تقليدها الكلاسيكية والمستحدثة لننتهي ببيان الفرق بينهما متتبعين في ذلك المنهج الوصفي والتحليلي للنصوص التي نظمت العلامة التجارية ، كما اعتمدنا على المنهج المقارن في بعض المواضيع التي ارتأينا فيها ضرورة اللّجوء إلى هذا المنهج.

المبحث الأول: ماهية العلامة التجارية

وفي هذا المبحث سنتعرض في المطلب الأول لمختلف التعريفات التي أسندها رجال الفقه والقانون للعلامة التجارية وللوظائف المختلفة التي أضحت تلعبها في الوقت الحالي الذي يشهد ثورة رقمية لا مثيل لها ، ثم نتعرض في المطلب الثاني إلى الإجراءات القانونية الواجب إتباعها لتسجيل العلامة التجارية تسجيلا رسميا يرتب كافة أثاره القانونية لمالكها .

المطلب الأول : تـــــعريف العلامة التجارية وأهميتها

الفرع الأول : تعريف العلامة التجارية

تعرف العلامة التجارية على أنها" السمة المميزة التي يضعها التاجر على منتجات محله التجاري ، أو الصانع على المنتجات التي يقوم بصنعها قصد تمييزها عن المنتجات الأخرى المشابهة لها في السوق، وكذلك السمة التي تستعملها مؤسسة لتقديم خدماتها" [1]، كما عرفها بعض الفقه بانها "أي إشارة ظاهرة يستعملها أو يريد استعمالها أي شخص لتمييز بضائعه أو منتجاته أو خدماته عن بضائع أو منتجات أو خدمات غيره" [2] ،كما عرفها البعض الأخر بأنها " الشكل والتكوين الخاص الذي

3- صالح فرحة زراوي، الكامل في القانون التجاري الجزائري، الجزء الأول،إبن خلدون للنشر والتوزيع ، الجزائر، 2001،ص208.

4: ا منة صامت ، الحماية الجنائية الموضوعية للعلامات التجارية –دراسة مقارنة ،الطبعة الأولى ،ريم للنشر والتوزيع ، السودان ، 2011،ص23.

يتخذه وسيلة لتمييز منتجات المشروع وخدماته " [1]،أو الشعار الذي يتخذه الصانع أو التاجر أو الزارع لمنتجاته أو بضائعه أو خدماته بحيث تضمن لمن يشتري بضاعة أصلها ومصدرها " [2].

أما المشرع الجزائري ،فقد عرفها في المادة 1/2 من الأمر 06/03 المؤرخ في 2003/07/19 المتعلق بالعلامات التجارية [3]والتي جاء فيها "... كل الرموز القابلة للتمثيل الخطي لاسيما الكلمات بما فيها الأشخاص والأحرف والأرقام والرسومات أو الصور والأشكال المميزة للسلع أو توضيبها ،والألوان بمفردها والمركبة التي تستعمل كلها لتمييز سلع أو خدمات غيره [4].

وقد نصت المادة01/03 من ذات الأمر على أنه "تعتبر علامة السلعة أو الخدمة إلزامية لكل سلعة أو خدمة مقدمة بيعت أو عرضت للبيع عبر أنحاء التراب الوطني "[5].

إذن وفقا لتلك التعريفات السابقة ،فإن العلامة التجارية هي "إشارة محسوسة توضع على المنتوج أو ترافقه ، أو الخدمة من أجل تمييزهم عن المنتوجات المشابهة للمنافسين أو الخدمات المقدمة من الآخرين "[6].

الفرع الثاني : أهميتها

إن الدور الذي تلعبه العلامة التجارية في تقدم ونمو المجتمعات قد جعلها تحظى باهتمام كبير من قبل رجال الفقه والقانون ولذلك فإن معظم التشريعات قد أحاطتها بعناية كبيرة من خلال مناداة أصحابها بضرورة تسجيلها تسجيلا رسميا على المستويين المحلي والدولي على حد السواء .

---

[1]: مختار محمود بربري ، قانون المعاملات التجارية ، الجزء الاول ،الطبعة الاولى ، دار النهضة العربية ، القاهرة، 2000،ص236

[6] ناهي صلاح الدين ،الوجيز في الملكية الصناعية والتجارية ،دار الفرقان ،عمان ،1983،ص233/منير محمود الجنيهي، ممدوح محمد الجنيهي العلامة التجارية والأسماء التجارية ،الجزء الأول ،دار الفكر الجامعي ،الإسكندرية ،2004،ص36.

[3]:ج.ر، العدد44 ، 2003/07/23، ص23.

[4] : حسين مبروك ، المدونة الجزائرية للملكية الفكرية ، الطبعة الأولى ،دار هومة للطباعة ، الجزاءر،2007،ص107

[5]: "السلعة هي كل منتوج طبيعي أوزراعي أو تقليدي خاما كان أو مصنعا ،أما الخدمة حسب نفس المادة فهي كل أداء له قيمة إقتصادية ".

[6]: Albert Chavannet jean-Jaques Burst,Droit de la propiete industriele, Delta,5éme edit,1998,P479.

كما أن كثرة الاتفاقيات الدولية المتعلقة بموضوع عناصر الملكية التجارية والصناعية يعكس مدى الاهتمام الدولي بموضوع الحماية القانونية للعلامة التجارية التي تلعب دورا هاما في تقدم وازدهار المجتمعات من الناحية العلمية ، الصناعية والتجارية[1] .

- هذا ويجمع الفقه على أن للعلامة التجارية دورا كبيرا في ترتيب علاقات الدول فيما بينها ،وخلق جو من التنافس الشريف بين الأفراد لأنها تعتبر إحدى الركائز التي يعتمد عليها نجاح أي مشروع إقتصادي ، وإحدى أهم القيم المضافة على رأسماله والتي من خلالها يستطيع التنافس مع غيره من المشاريع سواءا على الصعيد الدولي أو المحلي، كما أنها تعمل على جذب العملاء والمستهلكين مما يؤدي إلى رواج المنتجات والسلع محليا ودوليا ، وتحقيق الشهرة لمالكها ،وبالتالي العودة عليه بمردود مالي كبير وربح معنوي وفير خاصة إذا زاد تعلق المستهلكين بها لأن الدراسات والإحصائيات قد أثبتت أن زيادة تعلق المستهلكين بالمنتجات الحاملة للعلامة التجارية المشهورة يؤدي إلى الثبات في كمية المبيعات وإمكانية منح تراخيص بإستخدام تلك العلامة التجارية المشهورة مما يحقق لصاحبها أعلى قدر ممكن من الأرباح والفوائد.

إذن من خلال ماسبق يتضح أن للعلامة التجارية أهمية مزدوجة فهي من جهة تحقق مصالح طرفي العلاقة التجارية والصناعية لأنها تعتبر الوسيلة المثلى لتمييز السلع والمنتجات والخدمات عن غيرها من مثيلاتها مما يدفع المنتج أو الصانع أو مقدم الخدمة إلى محاولة إستقطاب أكبر عدد من المستهلكين عن طريق توخي الدقة والحرص على إبقاء درجة المنتج كما هي، أو تحسينها بشكل يعود على المستهلكين بالنفع ، وينعكس عليه إيجابا بسبب زيادة الطلب على منتجاته ويؤثر في زيادة الحركة التجارية و الإقتصادية في البلد الذي تستغل فيه هذه العلامة التجارية .

ومن جهة أخرى فهي تحقق مبتغى المستهلك في الحصول على بضاعة ذات جودة عالية تميزها عن غيرها من المنتجات المماثلة لها من حيث النوعية ،لأنه من خلال العلامة التجارية يستطيع المستهلك التعرف على مختلف السلع والخدمات المقدمة ليختار الأجود منها والأفضل لإستعمالها في مجالها المخصص لها بكل راحة وطمأنينة مادام أنه يثق في علامتها التجارية .

إذن وفقا للوظائف السابقة فإن العلامة التجارية تعتبر ضمانة قانونية لحماية المستهلك من الغش والتدليس الذي قد يلجأ إليه صاحب السلعة أو المنتج أو مقدم الخدمة لترويج بضاعته أو منتجه أو خدماته المقلدة أو المغشوشة ،أي التي تحمل مواصفات ناقصة أو مغايرة لمواصفات المنتجات

---

[1]1: حمادي زوبير ،الحماية القانونية للعلامة التجارية من الإعتداءات الواقعة عليها عبر شبكة الإنترنت ،الطبعة الأولى ،منشورات الحلبي الحقوقية ،بيروت 2012،ص19.

الأصلية وذلك طمعا في ترويج تلك المنتجات المغشوشة وذلك بدفع المستهلكين للإقبال عليها وشرائها ظنا منهم أنها تمتع بمواصفات المنتجات الأصلية ، وبالتالي تظهر الحماية الكبيرة التي توفرها هنا العلامة التجارية للمستهلك خاصة بالنسبة لفئة المستهلكين الواعيين أي الذين ينتبهون إلى أن السلعة المقلدة لاتحمل نفس العلامة المحفورة في السلعة الأصلية ،وبالتالي تكون العلامة التجارية هنا سببا في تجريم الغش والإحتيال في السلع والخدمات وتعريض مرتكبي هذه الجرائم للعقاب بسبب غشهم وخداعهم الموجه لمستهلكي السلعة أو البضاعة الأصلية [1].

المطلب الثاني : التنظيم القانوني للعلامة التجارية

لدراسة هذا النظام وجب علينا التعرض في فرع أول إلى نظام التسجيل التقليدي للعلامة التجارية ، ثم نظام التسجيل الإلكتروني لذات العلامة في الفرع الثاني .

الفرع الأول : التسجيل التقليدي للعلامة التجارية

يشترط القانون لإضفاء الطابع الرسمي على العلامة التجارية جملة من الشروط الشكلية و الموضوعية التي تجعلها قادرة على

تحقيق ذاتيتها ، وإكتسابها الشرعية التي تضفي عليها الحماية القانونية الكاملة ،والتي نوردها فيما يلي:

أولا : الشروط الموضوعية

وهي تتعلق بمجموعة من الشروط تخص شكل العلامة وهي كالتالي :

1-السمة المميزة للعلامة التجارية :

إن العلامة أيا كان شكلها أو صورتها يجب أن تتصف بصفات تعطي لها ذاتيتها الخاصة التي تميزها عن باقي العلامات الأخرى المستخدمة للسلع والخدمات المماثلة لها ،وهذا لمنع حصول اللبس لدى المستهلكين [2]،حيث يؤدي فقدان الصفة المميزة إلى رفض التسجيل طبقا لنص المادة07 من الأمر06/03 المؤرخ في 2003/07/19 المتعلق بالعلامات.

2-شـــــــــرط الجـــــــدة :

ويقصد به أن تكون العلامة التجارية جديدة في شكلها العام بحيث لم يسبق إستعمالها أو تسجيلها على نفس المنتجات أو البضائع أو الخدمات من طرف شخص اخر حتى لا تؤدي إلى التظليل

---

[1] : حسين فتحي،مرجع سابق ،ص10.

[2] : سميحة القليوبي ،الوجيز في التشريعات الصناعية ، الجزء الثاني ،دار النهضة العربية،القاهرة ،2007، ص72.

في أذهان الجمهور عند استعماله للمنتج فيختلط عليه الأمر مع علامة أخرى مشابهة لها [1]، والجدة المطلوبة المقصودة هنا هي الأسبقية من حيث طبيعة المنتجات المكان، والزمان[2] .

3-شرط المشروعية :

لا يكفي أن تكون العلامة مميزة وجديدة ،بل لابد أن تكون مشروعة أي غير مخالفة لنص أو أمر قانوني ، أو للنظام العام والآداب العامة ،وهذا ما أثبته المشرع الجزائري في نص المادة 07 من الأمر 03/06 المتعلق بالعلامات المنوه عنها أعلاه الذي يرفض تسجيل الرموز المخالفة للنظام العام والآداب العامة ،ومن ذلك حظر استعمال شعارات الملك العام أو السلطة العامة، والأعلام الوطنية كعلامات تجارية [3] .

ثانيا : الشروط الشكلية

إضافة إلى الشروط الموضوعية السابق التفصيل فيها ، لابد من توفر الشروط الشكلية التالية حتى تصبح العلامة متمتعة بالحق في الحماية القانونية وهي كالتالي :

1- إيداع طلب التسجيل:

ويتم هذا الإيداع طبقا لنص المادتين03و04 من المرسوم التنفيذي 277/05 المؤرخ في 2005/08/02 الذي يحدد كيفيات إيداع العلامات وتسجيلها والتي تنص على أنه يتم بموجب طلب يحرر وفقا للنموذج المحدد قانونا لدى المعهد الوطني الجزائري للملكية الصناعية الذي يقوم بفحص الطلب المودع من ناحية الشكل والمضمون ،ثم تقوم الهيئة المختصة بالمعهد بتحرير محضر يثبت تاريخ الإيداع ،ساعته ،ومكانه ،وكذا رقم تحرير التسجيل وهذا بعد دفع الرسوم المحددة في هذا الشأن ،ويعد هذا المحضر ذو أهمية بالغة لفض النزاعات التي يمكن أن تحدث مستقبلا بشأن تسجيل هذه العلامة التي قد يطالب بتسجيلها لأول مرة عدة أشخاص منفصلين.[4]

2- فحص التسجيل :

بعد قبول طلب الإيداع متى تم التأكد من إستيفائه لجملة الشروط الشكلية والموضوعية ،تقيد العلامة في سجل خاص بتقييد العلامات يمسكه المعهد وهذا طبقا لنص المادة 14 من المرسوم

[1] ناصر عبد الحليم السلامات،الحماية الجزائرية للعلامات التجارية ،دار النهضة العربية القاهرة،2008،ص133.

[2] :Ali Harou,La marque au magreb ,O.P.U ,Alger ,p72.

[16]: مصطفى موسى حسين العطيات ، التجارة الإلكترونية واثارها على إستخدامات العلامة التجارية ، رسالة دكتورة ، كلية الحقوق ،جامعة القاهرة،2008 ص198.

[4]: فرحة زراوي صالح ،مرجع سابق،ص34.

التنفيذي 277/05 الذي يحدد كيفيات إيداع العلامات وتسجيلها ، وتكون من اثار هذا التسجيل أن تصبح العلامة التجارية متمتعة بالحماية القانونية ،فيكون من حق مالكها إستعمالها، واستغلالها والتصرف فيها ،ومنع الغير من استعمالها دون ترخيص مسبق على سلع أوخدمات مماثلة أو مشابهة لتلك التي سجلت العلامة من أجلها،وله في ذلك أن يستعين بالقضاء طبقا لنص المادتين 28و29 من الأمر 03/06 المتعلق بالعلامات.

وتقرر هذه الحماية لمدة معينة تبدأ من تاريخ إيداع طلب التسجيل ،على أنه يستطيع مالك العلامة أن يستمر في التمتع بالحماية القانونية وذلك بتجديد تسجيلها لفترات متتالية[1] .

الفرع الثاني : التسجيل الإلكتروني للعلامة التجارية

تتم هذه العملية في الموقع الإلكتروني الذي تطلقه مصلحة تسجيل العلامات التجارية ،حيث يحدد هذا الموقع القواعد العامة التي يجب إتباعها في عملية التسجيل ،وذلك ببيان كيفية ملء الطلبات المعدة مسبقا في شكل نماذج إلكترونية وكيفية إرسالها إلكترونيا مرفقة بالوثائق المطلوبة إلى الموقع الذي يوفر خدمات البحث عن العلامات التجارية المتطابقة أو المتشابهة في قواعد بيانات دائرة التسجيل للتأكد من أن العلامة المراد تسجيلها غير مسجلة مسبقا ،أو متشابهة مع علامة أخرى مسجلة مسبقا .

و بعد إنتهاء عملية البحث ،و ثبوت جدية العلامة وباقي الشروط الواجب توفرها فيها كعلامة جديدة ،يتم قبولها ومطالبة مالكها بدفع رسوم التسجيل بإحدى طرق الدفع الإلكترونية المعتمدة من قبل الموقع ،وبعدها يتم إصدار الشهادات النهائية الخاصة بالتسجيل النهائي للعلامة التجارية، مع تبيان كيفية الحصول عليها طبقا لنص المادة16 من المرسوم التنفيذي 277/05 المنوه عنه أعلاه، وهنا ننوه أن السلطات المعنية لم تتمكن من حد الساعة إلى التطبيق المطلق لهذا النوع من التسجيل ،ولا زالت تعتمد على التسجيل التقليدي للعلامة التجارية .

إذن ، بعد إنتهائنا من تبيان طرق تسجيل العلامة التجارية ،أصبح بإمكاننا التعرض في الجزء الموالي للأساليب التقليدية والحديثة المعتمدة في تزوير العلامة التجارية .

المبحث الثاني : الأساليب المعتمدة في تقليد العلامة التجارية

---

[1]: فاضلي إدريس ، المدخل إلى الملكية الفكرية الأدبية والفنية الصناعية ،ديوان المطبوعات الجامعية، الجزائر، 2004، ص291.

وفي هذا المبحث سنتعرض في مطلب أول للأساليب الكلاسيكية التي كانت تعتمد في السابق في التعدي على معالم العلامة التجارية ، ثم نتعرض في مطلب ثاني لمعالم هذا التعدي الذي أصبح صارخا في ظل الثورة الرقمية التي تعيشها ساحة الإقتصاد الرقمي في الاونة الأخيرة .

المطلب الأول : الأساليب الكلاسيكية المعتمدة في التعدي على معالم العلامة التجارية

وسنتناول هذه الجزئية في ثلاث فروع أساسية سنتناول في الأول تزوير العلامة التجارية ، وفي الفرع الثاني تقليدها ،ثم ننتهي في الفرع الثالث إلى تبيان الفرق بينهما حسب الآراء الفقهية المتداولة .

الفرع الأول : تزوير العلامة التجارية

يفترض تزوير العلامة التجارية قيام المزور باصطناع علامة مطابقة تمام التطابق للعلامة محل التزوير بحيث يصعب التفرقة بين العلامة المزورة وتلك الأصلية ، وقد يقوم المزور أيضا بإنتزاع العلامة التجارية المطبوعة أو المرسومة أو المنقوشة على متن إحدى السلع أو المنتجات الأصلية ،ويضعها بدون ترخيص أو مبرر قانوني اخر على سلع أو منتجات أخرى .

إذن التزوير بهذا المفهوم هو نقل حرفي لعلامة تجارية بحيث يقوم المزور بإستخدامها لإصطناع علامة تجارية له بدون وجه حق ، أو قيامه بنقل وأخذ العلامة الأصلية بالكامل وإستخدامها دون مبرر قانوني على منتجات وبضائع أخرى غير تلك السلع والمنتجات التي سجلت رسميا بالأساس للدلالة عليها من خلال إعادة طبعها أو نقشها أو رسمها على سلعه أومنتجاته أو خدماته.

الفرع الثاني : تقليد العلامة التجارية

والمقصود به من الناحية الفقهية محاكاة العلامة التجارية المسجلة أو المستعملة من خلال إنشاء علامة تجارية تشابهها ولكن لا تطابقها تماما، أو تحاكي العناصر الرئيسية للعلامة دون أن تعتمد وتستغل هذه العناصر لتكوين علامة جديدة بحيث لو عرضت العلامتين معا لكنا أمام علامة أصلية ،وأخرى مصنوعة على غرارها.

فالتقليد بهذا المعنى يفترض بقاء العلامة المعتدى عليها كماهي دون إعتداء على مضمونها أو عناصرها الأساسية والإكتفاء بمحاكاتها أو تصنيع علامة أخرى على غرارها تأخذ من فكرتها الرئيسية أو تفاصيلها، عناصرها، أشكالها، وألوانها، ثم يتم صنع علامة أخرى تماثلها ولكنها تتطابق معها تماما لدرجة أنه فقط أصحاب الخبرة يستطيعون التمييز بين المنتج الأصلي والمقلد ، أما المستهلك العادي فإنه لايستطيع بخبرته المتواضعة إحصاء هذا التمييز ، وبالتالي من السهل جدا أن يقع ضحية لهذا التقليد .

الفرع الثالث : الفرق بين تزوير العلامة التجارية وتقليدها

من خلال ما سبق يتضح بأن هناك فرقا شاسعا بين التزوير والتقليد في العلامة التجارية ، فالتزوير يفترض نقل العلامة التجارية المسجلة نقلا حرفيا وتاما بحيث تبدو مطابقة تماما للعلامة الأصلية وبالتالي يفترض التزوير وجود إعتداء سواءا كان بشكل طابع أو حفر أو رسم ،وسم ، أو نقش لكامل العلامة التجارية محل التزوير أو على الأقل لأهم عناصرها الرئيسية ، ثم وضعها دون أي مبرر قانوني على سلع ومنتجات غير سلع ومنتجات مالكها الأصلي بقصد تظليل الجمهور والمستهلك وخداعه .

بينما التقليد فهو إتخاذ علامة تشبه في مجموعها العلامة الأصلية مما قد يؤدي إلى تظليل الجمهور أو خداعه ظنا منه أنها العلامة الأصلية، وقد توحد القضاء في موقفه بشأن التقليد من منطلق أنه لايستلزم أن يكون هناك تطابق تام بين العلامتين الأصلية والمقلدة ، بل يكفي لتوافر أركانه مجرد وجود تشابه بينهما من شأنه تظليل جمهور المستهلكين وإحداث اللبس بين السلعتين أو المنتجين أو البضاعتين .

إذن متى كانت العلامة مزورة، فإن الأمر لا يثير أي صعوبة لأن التشابه بين العلامة الأصلية والعلامة المزورة يكون تاما وهذا على خلاف التقليد الذي يقتضي إجراء المقارنة بين العلامتين لتحديد أوجه الشبه والإختلاف بينهما، وطبعا هذه المقارنة تحتاج إلى شخص خبير في الميدان لتأكيد حصولها وهو ما وضحه نص المادة34 من الامر06/03 المتعلق بالعلامات .

المطلب الثاني : الأساليب المستحدثة في تقليد العلامة التجارية

وسنتناول هذا الموضوع في فرعين أساسيين سنتناول في الأول نظرة عامة حول الجرائم المعلوماتية، ثم نتعرض في فرع ثان إلى أركان التقليد الإلكتروني للعلامة التجارية .

الفرع الأول : الجرائم المعلوماتية

لقد تعددت التعريفات التي تناولت الجريمة المعلوماتية فمنها من أعطاها تعريفا ضيقا كالفقهاء الفرنسيين ماس وستانت وفيفان[1] ، ومنهم من أعطاها تعريفا واسعا كالفقيهان كريدو وميشال[2]، كما تنافست الإتفاقيات الدولية والعربية على محاولة وضع تعريف جامع لها ، فقد عرفها خبراء متخصصون في بلجيكا في معرض ردهم على إستبيان منظمة التعاون الإقتصادي والتنمية

---

[1]: عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، الطبعة الأولى ،دار الفكر الجامعي ، مصر ،2006،ص98.

[2]: عرب يونس ، جرائم الكمبيوتر والأنترنت ،ورقة عمل مقدمة إلى مؤتمر الأمن العربي ،2002،ص4.

بأنها " **كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية** "، أما المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا في الفترة مابين 10إلى 17 أفريل 2000 فقد عرفها بأنها "**أية جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة إلكترونية** " [1]،أما الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها من قبل الجزائر في 2014 فقد إكتفت في الأحكام العامة من الفصل الأول بتعريف بعض المصطلحات في المادة الثانية كتقنية المعلومات ، مزود الخدمة ، البيانات ، البرنامج المعلوماتي ، النظام المعلوماتي ، الشبكة المعلوماتية...إلخ ، دون أن تضع أي تعريف لهذه الجريمة .

وعلى كل، فإن كل التعريفات التي أعطيت للجريمة المعلوماتية قد تعرضت للنقد على إعتبار أنها ناقصة ، وقد خلص الفقه إلى أنه للنجاح في وضع تعريف شامل للجريمة المعلوماتية لابد من مراعاة عدة إعتبارات مهمة منها مايلي [2]:

-أن يكون هذا التعريف مقبول ومفهوم على المستوين العالمي والمحلي [3] .

- أن يراعي هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات .

- أن يحدد التعريف الدور الذي قام به جهاز الكمبيوتر في إتمام النشاط الإجرامي .

-أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

-إن هذه الإعتبارات هي التي جعلت من وضع تعريف تشريعي ثابت للجرائم المعلوماتية يعتبر ضربا من المستحيل لاسيما وأن ثورة المعلومات، وتطور وسائل الإتصال التي أوجدت هذه الجرائم تشهد في كل ثانية تطورا مطردا لا سقف له ولهذا فقد عكفت معظم تشريعات العالم وعلى نحوها التشريع الجزائري على تجنب وضع تعريف لهذه الجريمة تاركة هذه المهمة للفقه[4].

---

[1]: زبيخة زيدان ، الجريمة المعلوماتية في التشريع الجزائري الدولي ، دار الهدى ، الجزائر ،2011،ص45.

:امال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ،،الطبعة الأولى ،دار هومة للطباعة والنشر ، الجزائر ، 2006، ص99.

[3]: هدى حامد قشقوش ،جرائم الحاسب الإلكتروني في التشريع المقارن ، الطبعة الأولى ،دار النهضة العربية، القاهرة ،1999،ص81.

[24]: عامر محمود الكسواني ، التزوير المعلوماتي للهلامة التجارية ،دراسة تحليلية تأصيلية مزودة ومدعمة بالإجتهادات القضائية ، دار الثقافة للنشر والتوزيع ،الاردن 2010 ،ص126.

وعلى كل ، فإن الجريمة المعلوماتية كغيرها من الجرائم لابد أن يتوفر فيها جاني ومجني عليه ،بالإضافة إلى الشروط العامة الواجب توافرها في مرتكب الجريمة المعلوماتية من سلوك منحرف مجرم قانونا، وعلم وإرادة واعية بنتائج هذا السلوك، غير أنه لابد أن يكون هذا الشخص على درجة معينة من العلم والخبرة والدراية الواسعتين في علم الحاسب وتقنية ، أو شبكة المعلومات ،وأن يكون محكوما برغبة جامحة في تحدي كل ماهو جديد ومبتكر ذلك أن معظم التحقيقات التي تتم مع هؤلاء الجناة الذين تم إلقاء القبض عليهم تسفر على أن سبب إرتكابهم لتلك الجرائم هو فقط تحدي وقهر أنظمة الحاسوب [1]،وهذا على عكس مرتكبي الجرائم الكلاسيكية الذين يرتكبونها في معظم الأحيان بدافع نفسي كالحقد والكراهية ، أو أسباب إجتماعية أو إقتصادية... إلخ

أما الفرق الثالث بينهما فهو أن مرتكبي هذه الجرائم المعلوماتية في معظم الأحيان يكون هدفهم مادي بحت بحيث يكون الهدف من هذه الجرائم جني أموال، ومكاسب كبيرة جدا[2] لاسيما وأنهم يستهدفون في معظم الأحيان المؤسسات المالية البنوك ، بنوك المعلومات والمصارف ، شركات الصرف ...إلخ

كان هذا عن أهم الصفات التي يتميز بها الجاني في هذا النوع من الجرائم ، أما عن المجني عليه في الجرائم المعلوماتية فهو في معظم الأحيان شخص معنوي كالمؤسسات العامة والشركات الإقتصادية الكبرى، والمنظمات والهيئات الحكومية وغير الحكومية، بالإضافة إلى الهيئات المالية الضخمة ،وغيرها من الأشخاص الإعتبارية التي تعتمد في إنجاز أعمالها على الحواسيب [3].

إن هذا الواقع الذي تثبته التجارب العملية لا يعني أن الشخص الطبيعي قد لا يقع ضحية للجريمة المعلوماتية، ولكنه يظهر أن الأشخاص الطبيعيين الذين يحفظون أسرارهم التجارية، وملفات أعمالهم داخل الحاسوب الشخصي أو المهني الخاص بهم هم الأكثر عرضة لهذا النوع من الجرائم.

---

[1]: نائلة محمد فريد قورة ، جرائم الحاسب الالي الإقتصادية ، الطبعة الاولى ،منشورات الحلبي الحقوقية ،لبنان، 2005،ص 58.

خالد محود إبراهيم ، الجرائم المعلوماتية ، الطبعة الأولى ،دار الفكر الجامعي ، الإسكندرية ، مصر ،2009، ،ص135. [2]

[27]: مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الإلكترونية ـدراسة مقارنة- دار النهضة العربية ، القاهرة، ص119 / هدى حامد قشقوش ،مرجع سابق ، ص6-18.

ويفترض أن يكون هؤلاء الأشخاص اللذين يجذب إليهم جناة الجرائم المعلوماتية ذوي مناصب سياسية أو قيادية رفيعة في الدولة ، أو رجال أعمال مرموقين ، أو أصحاب شهرة عالمية أو داخلية في أحد القطاعات الحساسة كتلك العسكرية الإقتصادية ، التجارية ، الإجتماعية ، الثقافية والعلمية ....إلخ [1]

هذا ، وتشير الدراسات الميدانية في هذا النوع من الجرائم أن تحديد نطاق خاص يضم كافة فئات الأشخاص المجني عليهم هو صعب نوعا ما في الجرائم المعلوماتية لأن هؤلاء المجني عليهم في الغالب لا يكتشفون هذه الجرائم إلا بعد تمام حصولها، الأمر الذي يدفعهم في غالب الأحيان إلى السكوت والإذعان وتفضيل هذا الموقف السلبي عن القيام بالتصريح عن تعرض المعلومات المخزنة في حواسيبهم للدخول غير المشروع ، والإنتهاك والقرصنة [2].

الفرع الثاني : أركان جريمة التقليد الإلكتروني للعلامة التجارية

- إن محل الجرائم المعلوماتية في إطار العلامات التجارية يكمن بالدرجة الأولى في عمليات التزوير والتقليد المرتكبة على العلامة التجارية المستخدمة من قبل صاحب الموقع الإفتراضي للدلالة على منتجاته وبضائعه ،وذلك من خلال العمل على نسخ وتقليد إحدى مضامين هذا الموقع الإفتراضي المتمثل بإحدى العلامات التجارية سواءا بالإضافة عليها، أو التقليل منها أو تشويهها مستغلين بذلك إقبال الأشخاص على إقتناء تلك السلع أو الخدمات بالذات لتعلقهم بعلاماتها التجارية، وإنحفارها في وجدانهم كوسيلة من وسائل معرفة وتحديد مصدر ومنشأ تلك السلع والخدمات. وعلى ما يبدو ، فإن المشرع الجزائري لم يتطرق بتاتا لمسألة التقليد الإلكتروني ،أو المعلوماتي للعلامة التجارية في الأمر06/03 المتعلق بالعلامات التجارية ، وإكتفى بالنص على جريمة التقليد الكلاسيكية للعلامة التجارية في نص المواد من 26 إلى المواد 33 من ذات الأمر ،وبالرجوع إلى قانون العقوبات نجد نص المادتين 394 مكررا1 و2 اللتان تعالجان موضوع التزوير والتقليد الإلكترونيين للمعطيات الإلكترونية بصفة عامة ،ولكن لا وجود لنص خاص بالعلامة التجارية.

---

[28]: طوني ميشال عيسى ، التنظيم القانوني لشبكة الإنترنت ، الطبعة الأولى ،دار صادر للمنشورات الحقوقية، بيروت، 2001،ص150 / يونس خالد عرب، مرجع سابق ،ص 203.

[29]: محمد حسام لطفي ، عقود وخدمات المعلومات ،دراسة في القانون المصري والفرنسي ،دار النهضة العربية للنشر والتوزيع ، القاهرة ،1994،ص109/ عامر محمود الكسواني ،مرجع سابق ، ص132.

كما أنه بتفحصنا للقانون09-04 المؤرخ في 2009/08/05 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها [1] فإننا لاحظنا أنه قد جاء خاليا من أي نص في هذا الشأن ،ولكن بالرجوع إلى الإتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر في 2010/12/21 فقد عرفت هذه الأخيرة في المادة 10 التزوير الإلكتروني كما يلي " هو إستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر ،وبنية إستعمالها كبيانات صحيحة "،غير أن المشرع الجزائري لم يدخل أي تعديل في هذا الشأن بعد مصادقته على هذه الإتفاقية على الأمر06/03 المتعلق بالعلامات التجارية مما يجعلنا نرتكز على نص المادة 10 من تلك الإتفاقية للقياس عليها في موضوع العلامة التجارية .

إذن من خلال دراسة هذا النص يتضح أن التقليد المعلوماتي هو الاخر كالتقليد الكلاسيكي يستلزم توافر ركنين أساسيين هما الركن المادي والركن المعنوي .

فأما **الركن المادي**، فإنه يمكن تحليله إلى ثلاث عناصر أساسية، وهي :

- محل جريمة التقليد وهو العلامة التجارية .
- النشاط الإجرامي المتمثل في فعل تحريف أو تغيير الحقيقة الواقعة على العلامة التجارية .
- الضرر كعنصر أساسي لايكتمل بدونه الركن المادي ، أما **الركن المعنوي** في التقليد المعلوماتي ، فهو الاخر يتحلل إلى عنصرين هما :

القصد العام : الذي بموجبه تتجه إرادة الجاني نحو إحداث الفعل الإجرامي المتمثل في تغيير الحقائق مع علمه بكافة عناصر الركن المادي لجريمة التقليد .

القصد الخاص : وهو أن تكون للجاني مرتكب التقليد نية أكيدة وهدف معين ،والمتمثل في إستعمال العلامة التجارية التي قام بتغيير حقيقتها ،وفيما يلي سنحاول التفصيل في كل عنصر من هذه العناصر على حدى .

أولا : الركن المادي :

إن المبدأ العام الذي يحكم جريمة التقليد ، و هو أن لا تقع هذه الأخيرة إلا بوجود علامة تجارية، فإذا انعدمت فلا وجود لهذه الجريمة لأن الهدف من تجريم التقليد هو : حماية المصحة العامة، وصيانة الثقة العامة بالعلامات التجارية ،وهو ما سنفصله فيما يلي :

1- وجود علامة تجارية إلكترونية مسجلة :

---

[1]: ج.ر ، العدد47، المؤرخ في 2009/08/16،ص5-8.

ويستوي في هذا الشأن شكل العلامة التجارية ،أو كيفية وضعها على السلعة فقد تكون مرسومة ،محفورة فيها أو مطبوعة ، أو مزيجا من ذلك كله ،وهذا بغض النظر عن المواد المستعملة في تشكيل العلامة.

كما لا يهم في هذا الشأن الدعامة التي تجسد فوقها العلامة التجارية فقد تكون على الورق، القماش ، الجلد ، الخشب الحديد ،أو غيرها من الدعامات الأخرى ،ولكن المهم أن تكون العلامة التجارية مسجلة وفقا للشروط والإجراءات القانونية التي بيناها سابقا حتى يستفيد مالكها من الحماية القانونية .

وقياسا على إعتبار المحررات المخرجة من أجهزة الحاسوب محررات معلوماتية ، فإن العلامة التجارية المخزنة داخل الحاسوب ، أو المعالجة اليا أو إلكترونيا ، أو المخرجة منه سواء عن طريق الطبع أو النسخ أو التخزين على قرص صلب ،أو أية دعامة الية أو إلكترونية حديثة تعتبر من قبيل المحررات الإلكترونية التي قد تخضع للتقليد مثلها مثل بقية المحررات الإلكترونية الأخرى، غير أنه يستوجب أن تتوفر في العلامة التجارية مجموعة من الشروط حتى تعتبر محررا إلكترونيا قد يتعرض للتقليد ،ومن بين هذه الشروط مايلي :

أ) - الوضوح الجلي لمالك العلامة التجارية :

والمقصود به ظهور واضح لمالك العلامة التجارية على سطح أو ظهر السلعة ، المنتج ، أو الخدمة أي الشخص الذي سجلت العلامة بإسمه سواء كان طبيعيا أو معنويا ،وهو الشخص الذي سيستخدم تلك العلامة التجارية في عملية التسويق لمنتجاته وسلعه بهدف الربح الوفير ، وهو ذاته الشخص الذي سمح لمنظم الموقع الإفتراضي الخاص به لمعالجة علامته التجارية إلكترونيا ،ووضعها على موقع أعماله على شبكة الإنترنت ، لأنه متى إستحال أو تعذر تحديد مصدر العلامة إنتفت عن الكتابة فكرة المحرر الذي يصلح محلا لجريمة التقليد .

كما أن إشتراط إظهار مالك العلامة التجارية فيها حتى تعتبر هذه الأخيرة محلا صالحا لأن يكون محلا لجريمة التقليد لا يعني إطلاقا أن تكون العلامة مذيلة بتوقيعه أو ختمه ،بل يكفي في هذا الصدد إمكانية الإستدلال على شخصية المالك من واقع الحال ،أو من خلال بيانات وعلامات خاصة بمالك العلامة التجارية التي تدل دلالة قاطعة على نسبة العلامة له،وهذا ما يستشف ضمنيا من خلال نص المادتين 28و29 من الأمر 06/03 المتعلق بالعلامات.

ب)- مضمون العلامة التجارية :

لابد أن تكون العلامة التجارية متكونة من مجموعة من الأفكار المترابطة ،أو الألوان المتناسقة فيما بينها والتي قد تتكون من أرقام ،أو حروف، أو كلمات ،أو عبارات مترابطة تعطي معنى مفهوم للناس ،وبالتالي فإن تغيير الحقيقة في هذه المعاني والأفكار والألوان ، أو الكلمات أو الحروف أو الأرقام يؤدي بدون شك إلى قيام جريمة التقليد لاسيما إذا كانت هذه العلامة معالجة قبل إصدارها عن طريق الحاسوب ،وموضوعة أو مخزنة أو مسجلة على موقع إفتراضي من المواقع الخاصة بالأشخاص والشركات التجارية المنتشرة عبر صفحات الإنترنت.

2- تغيير الحقيقة الواقعة على العلامة التجارية بإستخدام وسائل تقنية المعلومات بنية إستعمالها كعلامة صحيحة :

إن هذا النشاط الإجرامي يشكل الركن الأساسي في قيام جريمة تقليد العلامة التجارية ،لأن هذه الجريمة لا تقوم أصلا إلا إذا حدث تغيير للحقيقة في جوهر العلامة التجارية ،وعناصرها الأساسية بحيث يتم إستبدال هذه العلامة بما يغايرها وذلك عن طريق الزيادة أو الحذف من عناصر هذه العلامة التجارية سواء كانت أرقاما ، أو صورا، أو أشكالا موجودة فيها بحيث يترتب عليها خلق علامة تجارية جديدة ،أو تضخيم العلامة التي كانت موجودة فوق السلعة أو المنتج أو الخدمة ،أو تحريفها ،أو تخفيضها أو تدقيقها على نحو تصبح فيه أكثر حسما عند الإحتجاج بها أو إسنادها إلى غير مصدرها.

كما يشترط أن يكون التغيير قد وقع على العلامة التجارية بعد تسجيلها تسجيلا رسميا لتمييزها عن باقي المنتجات السلع والخدمات المشابهة لها داخل بلد الحماية ،وألا يكون قد وقع التقليد قبل تسجيل العلامة ،أو بعد إنتهاء مدة الحماية القانونية الممنوحة لها بموجب شهادة التسجيل، وعدم القيام بتجديد هذه العلامة ،وهو ما أكده نص المادة01/27 من الامر 06/03 المتعلق بالعلامات .

كما يشترط في هذا التحريف أيضا أن يكون قد تم خلافا لإرادة المالك ،أ و صاحب العلامة التجارية ، أي بدون طلب أو رخصة منه ،وخلافا لأحكام القواعد والإجراءات الخاصة بتسجيل العلامات التجارية .

هذا وقد إتفق القضاء على أنه لا يشترط أن يكون التزوير أو التحريف الواقع متقنا أو غير ظاهر أو محكما ، أو قد تم بمهارة ودقة ، بل يكفي أن تكون العلامة التجارية المقلدة ذات مظهر يمكن أن يخدع به جمهور المستهلكين المقبلين على المنتج أو السلعة ذات العلامة

الأصلية ،وهذا ما يستشف من نص المادة210 من قانون العقوبات الجزائري ، كما أن الأمر يتطلب بحسب الخبراء أن يكون في الأمر تشابه يدخل به الغش على الأفراد ،ويؤدي إلى تظليل الجمهور، أي أن يكون في نية المقلد التظليل [1] .

إذن، من خلال ما سبق يتضح أن المقصود بتغيير الحقيقة الواردة على العلامة التجارية إلكترونيا لابد أن يتمثل في نقل أو أخذ أو إنتزاع كامل العلامة التجارية المسجلة تسجيلا صحيحا وقانونيا بحيث يكون منتجا لكافة اثاره أو نقل أو أخذ أو إنتزاع أحد عناصر العلامة المسجلة ،ووضعها دون وجه حق على بضائع أو سلع أومنتجات أخرى الأمر الذي قد يوحي دون حق بأن العلامة المقلدة تطابق العلامة الأصلية ،أو أن المنتجات أو السلع أو البضائع التي قد تم وضع العلامة المقلدة عليها عنوة، ودون وجه حق هي نفسها المنتجات والسلع والبضائع التي تحمل العلامة الأصلية المعتدى عليها، على أن يتم هذا التقليد والتغيير بإستعمال وسائل الإتصالات ونقل المعلومات الحديثة.

إن هذا التغيير قد يتم أيضا من خلال نقل هذه العلامة عن الموقع الإلكتروني المفتوح من قبل صاحب العلامة ووضعها اليا وإلكترونيا دون أي مبرر قانوني على موقع اخر غير مملوك لصاحبها ، أو من خلال إعادة نسخها أو تخزينها أو تصويرها أو إستعمالها دون وجه على غير المنتجات أو السلع التي سجلت عليها العلامة من قبل ، أو من خلال تغيير حقيقتها المطبوعة أو المخزنة في الحاسوب أو الديسكات أو الأقراص المدمجة أو الممغنطة أو غيرها من الدعامات والوسائل المعلوماتية المستحدثة في أنظمة الحاسوب ،ثم طبعها وإخراجها من الحاسوب والتلاعب بها بعد ذلك دون وجه حق في التدليس والتحايل وخداع الأفراد [2].

هذا ، وقد أثارت مسألة الشروع في التقليد المعلوماتي للعلامة التجارية جدلا فقهيا كبيرا ، أي أنه متى تمت المعالجة الالية والإلكترونية للعلامة التجارية المخزنة داخل الحاسوب بدون أي مبرر قانوني،ثم لم يتم إستعمال العلامة التجارية المعالجة إستعمالا خارجيا ، أي لم يتم إخراجها من الحاسوب وإستعمالها ،فما هو الجزاء المترتب على ذلك ؟

---

[1]: عبد الفتاح البيومي ، الدليل الجنائي للتزوير في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، القاهرة، 2002،ص137.

[2]: فوزية عبد الستار ، شرح قانون العقوبات – القسم الخاص – دار النهضة العربية ، القاهرة، 1988، ص244.

لقد إنقسمت التشريعات في هذا الشأن إلى فريقين حيث تنص بعض التشريعات بأن تغيير الحقيقة في العلامة التجارية دون أي مبرر قانوني كاف لوحده لقيام جريمة التقليد المعلوماتي لأن الشروع في الجريمة يعرف فقهيا وقانونيا وقضائيا بأنه البدء في تنفيذ الأفعال الظاهرة المؤدية إلى إرتكاب جناية أو جنحة ،و هو الطرح الذي تبناه المشرع الجزائري في نص المادة 394 مكرر7 من قانون العقوبات[1]،ونص المادتين 28و29 من الأمر 06/03 المتعلق بالعلامات ، في حين نصت تشريعات أخرى كالتشريع الأردني الذي سايره قضائه في العديد من قراراته بأنه متى لم يتم إستعمال العلامة التجارية المقلدة إلكترونيا إستعمالا خارجيا على وجه غير مشروع يضر بالغير ،فإنه لا يمكن إعتبار ما صدر من المقلد المعلوماتي بدءا في تنفيذ جناية أو جنحة التزوير ، بل يعتبر ذلك من قبيل الأعمال التحضيرية فقط لأن العنصر الأساسي في هذه الجريمة وهو" الضرر" لم يتحقق بعد[2].

أما إذا تم خلق علامة تجارية بأكملها عن طريق التقليد إستنادا إلى علامة أصلية ،ونسبها زورا إلى شخص اخر غير مالكها ، فنكون هنا أمام جريمة تزوير تامة الأركان يستوجب معاقبة فاعلها مع شركائه إن وجدوا لأنها ستسبب ضررا جسيما لمالكها، وهو ما سنتناوله في الموالي.

3- الضـــــــــــــــرر :

يعتبر الضرر عنصرا أساسيا في جريمة التقليد المعلوماتي للعلامة التجارية لأنه بإنعدامه تنعدم الجريمة دون الحاجة للبحث عن توافر الأركان الأخرى لهذه الجريمة ، مما جعل البعض يعتبره ركنا مستقلا بذاته في هذه الجريمة[3] ، والضرر كما عرفه البعض هو " إهدار لحق أو مصلحة يحميها القانون نتيجة تغيير حقيقته " ،وبالتالي فإن الضرر المقصود هنا هو الضرر بمفهومه الواسع الذي يتحقق في كل تغيير للحقيقة، متى ترتب عليه إهدار لحق معين ،أو مصلحة معينة يحميها القانون ،وبصرف النظر عن شخص ذلك الحق أو تلك المصلحة [4].

إن الضرر بهذا المعنى يتسع ليشمل الضرر المادي ، المعنوي أو الإجتماعي الذي يترتب على مجرد العبث في المحررات بصفة عامة والعلامات التجارية بصفة خاصة مما يسقط ثقة المجتمع

---

[1]: " يعاقب بالشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "

[34]:عامر محمود الكسواني ،مرجع سابق ، ص220.

[3]: محمد نجيب حسني ، شرح قانون العقوبات –القسم الخاص ،دار النهضة العربية ، القاهرة ،1988،ص282.

[36]: امال عبد الرحيم عثمان ،شرح قانون العقوبات –القسم الخاص –الجرائم المخلة بالثقة العامة ،مطابع الهيئة المصرية العامة للكتاب ، مصر ،1989 ص366.

بشأنها "[1] ، بالإضافة إلى الضرر البسيط والجسيم ،وفيما يلي سنتفصل في كل صورة من هذه الصور :

- الضرر المادي والمعنوي :

يتفق الفقهاء على تعريف الضرر المادي بأنه" ذلك الضرر الذي يصيب الذمة المالية للشخص بمعنى ذلك الضرر الذي يؤدي إلى تخفيض مستوى الحقوق وزيادة مستوى الإلتزامات ".

- ويعتبر الضرر المادي هو الأكثر شيوعا في جرائم التقليد الإلكتروني للعلامة التجارية لأن هذه الأخيرة قد أصبحت مؤخرا أهم وأكبر قيمة مضافة على رأسمال المشروع ، وبالتالي فإن تقليدها يترتب عنه دون أدنى شك ضرر مادي جسيم بالنسبة لمالكها الذي يكون قد أنفق في الكثير من الأحيان مبالغا قد تكون خيالية على الدعاية والإعلان من أجل الترويج لتلك العلامة التجارية ، كما أنها تؤثر على السمعة التجارية لمالك العلامة التجارية وهيبته خاصة إذا كانت العلامة التي تعرضت للتقليد ذات شهرة تخطى الحدود .

إن هذا التأثير قد يؤدي إلى الحط من قيمة السلعة أو البضاعة محل العلامة التجارية المقلدة، ونفور الزبائن عنها نفورا نسبيا أو كليا مطلقا ،وهو الضرر الذي يتحقق فعلا في الكثير من الأحيان[2].

كما قد يصاحب هذا الضرر المادي ،ضرر معنوي أو أدبي وهو الذي يلحق مالك العلامة التجارية في شرفه وكرامته وعرضه كأن يتم المساس بالمكانة الإجتماعية لمالك العلامة ، فيتم إقصاؤه من بعض النوادي ،أو بعض المجمعات المالية التي كان ينتمي إليها بسبب سعة شهرته التي تسبب فيها رواج علامته التجارية التي تعرضت للتقليد .

ولنا أن نتصور أيضا في هذه الصورة الضرر الإجتماعي المترتب من جراء هذه الجريمة كما نوهنا عنه سابقا لأن تغيير حقيقة علامة تجارية إلكترونيا بدون أي مبرر قانوني سيؤدي بدون أدنى شك إلى الإخلال بمستوى الثقة العامة المقررة للعلامات التجارية المسجلة إلكترونيا بصفة خاصة ،والمحررات الإلكترونية بصفة عامة خاصة بالنسبة للدول التي قد تخلت في أنظمتها القانونية على التطبيقات التقليدية، وإستعانت بالتطبيقات الإلكترونية الحديثة في جميع المجالات الإقتصادية والتجارية كالولايات المتحدة الأمريكية، الصين، والكثير من الدول الأوروبية.

---

[1]: محمد زكي أبو عامر ، قانون العقوبات – القسم الخاص ، الدار الجامعية ، لبنان ، 1989،ص121.

[2]: عمر السعيد رمضان ،شرح قانون العقوبات –القسم الخاص ،دار النهضة العربية، القاهرة،1987 ، ص123.

ولتلك الأسباب فقد إستقر الفقه والقضاء في تلك الدول على أن القاضي الذي ينظر النزاع الذي يكون محله علامة تجارية مقلدة إلكترونيا لا يجب أن يجبر الضرر الفردي لمالك العلامة المزورة إلكترونيا فقط ، بل عليه أن يجبر أيضا الضرر الإجتماعي الذي يفقد المستهلكين الثقة العامة في العلامات التجارية المسجلة تسجيلا رسميا[1].

أما عن **الضرر المحتمل** في هذا النوع من الجرائم ، فقد عكف الفقه إلى القول بأن جريمة تقليد العلامة التجارية إلكترونيا تقع حتى ولو حالت ظروف معينة دون وقوع الضرر بالفعل، حيث يكفي أن يكون حدوث الضرر محتمل الوقوع وقت حدوث فعل تغيير الحقيقة في العلامة التجارية لخطورة هذه الجريمة، ووقعها السلبي على التجارة الإلكترونية [2].

ثانيا : الركن المعنوي في جريمة التقليد المعلوماتي للعلامة التجارية

ويتمثل في الإحتيال أو الخداع الذي يعتبر من الأركان المفترضة ، حيث لا تقع هذه الجريمة إلا إذا تمت بسوء نية ، أما إذا تمت بحسن نية فلا عقاب عليها لأن تزوير العلامة التجارية إلكترونيا لا يقع إلا تحقيقا لهدفين هما:

- التعدي على العلامة التجارية إلكترونيا .
- خداع المستهلك وتظليله [3].

وعلى كل ،فإن هذا الركن يمكن استخلاصه من مجموعة من القرائن والوقائع خصوصا إذا كان المقلد تاجرا ،أو شركة تجارية ،حيث يعتبر سوء النية لديهما مفروض وليس مشروط[4].

وطالما أن نية الاحتيال في تزوير العلامة التجارية إلكترونيا هو مفترض ، فإن هذا يجعل هذه الجريمة من قبيل الجرائم القصدية التي تستلزم توافر القصد العام والقصد الخاص ،وهو ما سنفصله فيما يلي :

1- القـــــصد العـــــــــــــــــــام :

[1]: عامر محمود الكسواني ، مرجع سابق ،ص216.

[2]: إيهاب فوزي السقا ، جريمة التزوير في المحررات الإلكترونية ،دار الجامعة الجديدة للنشر ، الإسكندرية ، 2008،ص57.

[3]: صلاح زين الدين ، الملكية الصناعية والتجارية ،دار الثقافة للنشر والتوزيع، الأردن، 2000، ص403.

[4]: عبد الحكيم فودة ،جرائم الغش التجاري والصناعي ،منشأة المعارف ، الإسكندرية ،1996،ص13.

ويقصد به أن تتوفر لدى المزور إرادة القيام بتغيير حقيقة العلامة المسجلة[1]، لأنه بمجرد تسجيل العلامة التجارية تسجيلا رسميا ،فإنه لا يجوز لأي شخص الإعتذار بجهله لواقعة تسجيلها ،ولهذا فإن واقعة سوء النية في المعاملات التجارية تعتبر من قبيل الأمور المفروضة وليست المشروطة .

إن هذا المعنى يقودنا إلى القول بأن التاجر أو الصانع أو مقدم الخدمة يفترض علمه بواقعة تسجيل العلامة التجارية فإذا قام بتقليدها إعتبر سيئ النية ، ولا يطلب من مالك العلامة التجارية المسجلة رسميا بطريقة إلكترونية أو تقليدية إثبات سوء نية المزور ، وهذا مايستشف من نص المواد29،28و30 من الامر 06/03 المتعلق بالعلامات .

كما أن علم المقلد بوسائل وطرق التقليد كإصطناع أو حفر، أو رسم أو وشم أو طبع أو لصق هذه العلامة المسجلة بإسم شخص اخر ، ثم إستعمالها دون وجه حق على منتجات أوسلع أخرى يعتبر من الأمور المفترضة حيث لا يكن في أي حال من الأحوال أن يتذرع المقلد بجهله لهذه الوسائل لأنها مجرمة قانونا ، ولا أحد يعذر بجهله للقانون[2] .

2- القصد الخاص :

إن القصد العام في جريمة التقليد المعلوماتي هو غير كاف ، بل لابد أن يتوفر لدى المقلد قصد خاص بمعنى أن تتجه إرادته لحظة إرتكاب فعل تغيير حقيقة هذه العلامة إلى تحقيق غاية معينة ألا وهي إستعمال العلامة المقلدة إستعمالا يحقق الغاية التي ينشدها المزور من وراء فعل التقليد ،أي أن يتم إستعمال العلامة التجارية المقلدة و المسجلة مسبقا تسجيلا رسميا سواءا كان تقليديا أو إلكترونيا من قبل المقلد على سلع وبضائع أخرى غير تلك التي تم إستعمال العلامة التجارية من قبل عليها بقصد الربح ،أو الإضرار بمالكها[3].

وبمفهوم المخالفة ، فإن تزوير العلامة التجارية معلوماتيا لمجرد إثبات قدرة المزور وكفائته في التزوير ،أو من أجل المزاح مع صاحب العلامة أو مالكها، أو غير ذلك من الحالات لا

---

[1]: مأمون محمد سلامة ، قانون العقوبات –القسم العام –الطبعة الثالثة ،دار الفكر العربي، الإسكندرية،1990، ص116.

[2]: عمر سالم ، الحماية الجنائية لبطاقات الإئتمان –دراسة مقارنة- الطبعة الأولى ، دار النهضة العربية ، القاهرة، 1995 ،ص82.

[45]: عمر السعيد رمضان ،مرجع سابق ،ص 205.

تقوم معها جريمة التقليد المعلوماتي لإنتفاء النية في إستعمال العلامة التجارية المزورة فيما زورت من أجله.

وعلى كل ،فإن مسألة ثبوت توفر القصد الجنائي الخاص لدى المقلد من عدمها تعتبر من المسائل الموضوعية التي يستقل ببيانها وإثباتها قاضي الموضوع ،بحيث أن له أن يستخلص وجودها من خلال الأدلة والقرائن المعروضة أمامه دون أن يكون عليه أية رقابة طالما أن إستخلاصه لهذا القصد كان إستخلاصا سائغا، فإذا ثبت هذا القصد الخاص إلى جانب القصد العام في المتهم عوقب بنص المادة 32 من الامر 06/03 المتعلق بالعلامات التي تقضي بالعقوبة الأصلية المتمثلة في الحبس والغرامة أو بإحدى هاتين العقوبتين ،إلى جانب العقوبات التكميلية المتمثلة في الغلق النهائي أو المؤقت للمؤسسة المتابعة بالتقليد ،مع مصادرة الأجهزة والحواسيب وكل وسائل تقنية المعلومات التي تمت بموجبها عملية التقليد مع إتلافها بإعتبارها محل المخالفة طالما أن المشرع الجزائري لم يفرق بين جريمتي التقليد الكلاسيكية والمعلوماتية وهذا وفقا لنص المادة 5 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها من قبل الجزائر التي جاء فيها مايلي "تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل وفقا لتشريعاتها وأنظمتها الداخلية " .

الخـــــــاتـــــــمة :

لقد أصبحت العلامة التجارية تلعب دورا كبيرا في نمو وتقدم المجتمعات حيث أصبحت حاليا تعتبر معيارا إقتصاديا هاما يقاس به تقدم معالم الدول أو تخلفها ،وهو ماجعل التشريعات الداخلية والدولية توليها إهتماما فائقا خاصة بعد كثرة تعرضها للتقليد والتزوير، حيث أن هاتين الجريمتين لم يعد إرتكابهما بالأسلوب التقليدي المعروف ،وإنما أصبحت الوسائل التكنولوجية والآلية والرقية من أهم الوسائل المستحدثة التي تستعمل في تغيير حقيقة معالم العلامة التجارية بهدف تحقيق الربح الوفير على حساب تظليل جمهور المستهلكين وخداعه ،وهو ما فصلنا فيه في هذه الدراسة التي خلصنا فيها إلى النتائج التالية :

- إن العلامة التجارية المخزنة داخل الحاسوب،أو المعالجة اليا والكترونيا ،أو المخرجة منه سواءا عن طريق الطبع ،أو النسخ أو التخزين على قرص صلب ،أو أية دعامة الية أو إلكترونية حديثة تعتبر من قبل المحررات الإلكترونية .

- إن التسجيل الإلكتروني للعلامة التجارية لا يتعارض في مضمونه مع التسجيل التقليدي لأن كلاهما يتم وفقا للأنظمة القانونية للتسجيل ،ولا يظهر الإختلاف بينهما إلا من حيث

الالية الإلكترونية التي يعتمد عليها التسجيل الإلكتروني للعلامة التجارية بحيث يكون لهذا النوع من التسجيل نفس الاثار القانونية للتسجيل الورقي ، غير أنه يتميز عنه بكونه فيه إختصار كبير للوقت والمصاريف مما يجعلنا نناشد المشرع الجزائري لتوظيفه إداريا كوسيلة رقمية مستحدثة إلى جانب اليات التسجيل التجاري الإلكتروني الأخرى .

- إن تقليد العلامة التجارية إلكترونيا يعد نموذجا صارخا للجرائم المعلوماتية وهي لا تختلف عن جريمة التقليد الكلاسيكية لا من حيث الأركان ولا الشروط ،ولا من حيث صور التقليد ، ولكن الفرق بينهما يظهر في الوسيلة المستعملة في التقليد ألا وهي الوسائل الرقمية والإلكترونية .

- لابد على المشرع الجزائري أن يتأقلم مع جملة الاليات المستحدثة التي نتجت عن الثورة الرقمية والإلكترونية ، ولهذا ندعوه من هذا المنبر إلى ضرورة تحيين القانون المتعلق بالعلامات الذي لم يتعدل منذ حوالي 17 سنة ،مع ضرورة إفراد نصوص خاصة ودقيقة فيه تعالج جريمتي التقليد والتزوير التي أصبحت تطول العلامات التجارية اعتمادا على الوسائل الرقمية والإلكترونية .

الحماية الجنائية للمستهلك الإلكتروني من جريمتي الغش و الخداع

Criminal protection for the electronic consumer from the crimes of fraud and deception

د. ليطوش دليلة أستاذة محاضرة قسم أ
جامعة الإخوة منتوري قسنطينة 1- الجزائر

مقدمة:

لقد أصبحت حاليا معظم المجالات الحيوية تعتمد على الكمبيوتر، فقد تطورت مفاهيم جديدة منها الإنترنت الذي أصبح الشريان الرئيسي للإمداد المعلوماتي، و من الطبيعي أن يصاحب هذا التطور الذي اكتسح مجالات حياتنا اليومية و خصوصا منها التجارية عدة مشاكل و سلبيات خصوصا على صعيد هذه التعاملات التي تتسم بطابع مادي يغلب عليه حب الكسب المالي، فالمستهلك أحيانا لا يستطيع تلبية حاجاته إلا عن طريق التجارة الإلكترونية و هنا يصادف نوعا خاصا من المجرمين الذي يوقعون عليه أنواعا شتى من الغش و الخداع و ذلك في سبيل الوصول إلى غاياتهم الخاصة ألا و هي تحقيق الربح بطرق غير مشروعة.

فإذا كانت أشكال الغش و الخداع التقليدية المعروفة تهدد المستهلكين أفرادا و مؤسسات، فإن التطور المعلوماتي جاء بأعباء إضافية تلزم توفر التحكم في التقنية العالية لحماية المستهلك الذي في غالب الأحيان لا يملك سوى ثقافة بسيطة حول المعلوماتية و آلية التحكم في الإنترنت.

و من هنا راودنا التساؤل حول الحماية الجنائية التي يوفرها المشرع الجزائري للمستهلك الإلكتروني من جريمتي الغش و الخداع ؟

و من أجل الإجابة عن هذا التساؤل اعتمدنا على المنهج التحليلي و الوصفي من أجل الإلمام و تحليل ما توصل إليه الفكر التشريعي و الفقهي حول الموازنة بين التطور التكنولوجي الذي أدى إلى ولوج الأفراد الطبيعيين و المعنويين عالم التجارة الإلكترونية و كيفية حمايتهم جزائيا من شتى صور الغش و الخداع.

قد قسمنا هذا البحث إلى محورين يتناول المحور الأول: النطاق العام لجريمتي الغش و الخداع، و يتناول المحور الثاني: إجراءات حماية المستهلك الإلكتروني من جريمتي الغش و الخداع والعقوبات المرصودة.

المحور الأول: النطاق العام لجريمتي غش و خداع المستهلك الإلكتروني.

يتعرض المستهلك الإلكتروني للغش و الخداع في مواجهة التعاملات غير المشروعة من المحترف و بغاية الكسب السريع، هذا الأخير الذي يسخر فنياته و كل ما هو متاح على صعيد التجارة الإلكترونية لخداع المستهلك الإلكتروني المتعامل معه.

أولا: الإطار المفاهيمي لعناصر الموضوع.

إن هذا الموضوع له من الأهمية التي تجعلنا نتقصى عن حيثيات كل لفظ و معناه لأنه بفهم كل فكرة على حدا نستطيع فهم مجموعها، فلفظ الغش و الخداع متقاربان من حيث أن كلاهما يشكلان فعلا غير مشروع اعتاد الفكر على جعلهما في خانة المحظورات، و لكن يتعسر على غير المتخصص معرفة كيفية وقوعهما على من يسمى بالمستهلك الإلكتروني و هذا الأخير يشابه المستهلك التقليدي في كل السمات عدا أنه يتعامل عبر الوسائط الإلكترونية و الإنترنت، ما فرض على المشرع إفراده بخصوصيات معينة تميزه عن المستهلك التقليدي.

1: مفهوم جريمة الغش و الخداع.

يعتبر الغش و الخداع من الآفات الاجتماعية المعاصرة التي تستفحل في مجتمعاتنا و تمس بأمننا و سلامة المستهلك الإلكتروني، و يعرف الغش على أنه : "كل لجوء إلى التلاعب و المعالجة غير المشروعة التي لا تتفق مع التنظيم و تؤدي إلى التحريف في التركيب المادي للمنتج، و يتخذ النشاط المادي للغش إما شكل الإضافة أو الإنقاص أو الاستعاضة أو التحريف"[1].

و يعرف الغش أيضا بأنه: "كل فعل من شأنه أن يغير من طبيعته، أو خواص المواد أو فائدتها التي دخل عليها عمل الفاعل "[2].

أما جريمة الخداع فتتمثل في: " استعمال حيلة توقع المتعاقد في غلط يدفعه إلى التعاقد "[3]، ويعرف أيضا بأنه: " القيام بأعمال و أكاذيب من شأنها إظهار الشيء على غير حقيقته أو إلباسه مظهرا يخالف ما هو عليه في الحقيقة و الواقع"[4] .

---

[1]. أكسوم عيلام (رشيدة) : المركز القانوني للمستهلك الإلكتروني، مذكرة لنيل درجة الدكتوراه، جامعة مولود معمري، تيزي وزو، 2018، ص 390.

[2]. الغش التجاري في المجتمع الإلكتروني، مداخلة مقدمة إلى الندوة الرابعة لمكافحة الغش التجاري و التعليمي في مجلس التعاون الخليجي خلال الفترة 20 – 21 سبتمبر 2005، بعنوان: ظاهرة الغش التجاري و التقليد في ظل التقني و التجارب العالمية المعاصرة، إعداد مركز البحوث و الدراسات، ص 10.

[3]. أكسوم عيلام (رشيدة) : المرجع نفسه، ص 391.

[4]. المرجع نفسه، ص 391.

فقد يلجأ المحترف عامدا لأجل الترويج لمنتجاته إلى الدعاية المضللة التي قد تنطوي في بعض الأحيان على مغالطات علمية بهدف تحقيق الربح على حساب المستهلك الإلكتروني الذي تخدعه هذه الدعاية، و منها أيضا ما تلجأ إليه شركات صناعة الألبان المجففة من دعاية عبر شبكة الإنترنت و غيرها تفيد أن منتجاتها هي البديل الكامل للبن الأم على حين أن الثابت لدى منظمة الصحة العالمية أن ملايين الأطفال خاصة في دول العالم الثالث يموتون سنويا قبل السنة الأولى من أعمارهم بسبب اعتمادهم في التغذية على الألبان الصناعية[1]، و لو أن هذا النوع من الخداع يطال المستهلك العادي و المستهلك الالكتروني معا.

2: مفهوم المستهلك الإلكتروني.

لقد برز مؤخرا الاهتمام الكبير من طرف المشرع الجزائري للمستهلك عموما و المستهلك الإلكتروني على وجه الخصوص خصوصا في ظل جملة القوانين التي اعتمدها كقانون حماية المستهلك و قمع الغش، الحامل لرقم 03/09 [2] المعدل بموجب القانون 09/18 المؤرخ في 10 /2018/07.

و كذلك القانون المتعلق بتنظيم التجارة الإلكترونية رقم 05/18 المؤرخ في 2018/05/10، و غيرهما من القوانين إضافة إلى ما أورده بموجب أحكام قانون العقوبات الجزائري الذي تمثل أحكامه أعلى درجات الحماية القانونية التي أوجبها المشرع الجزائري للمستهلك الإلكتروني خصوصا و كل المتعاملين في الشق التجاري على اختلافهم بوجه عام، خصوصا و أن هذا الأخير تقوم دعائمه دائما على فكرة السرعة و الثقة و الائتمان.

و قد اختلف فقهاء القانون في وضع مفهوم موحد **للمستهلك** عموما فهناك من عرفه بأنه: "من يقوم باستعمال السلع و الخدمات لإشباع حاجياته الشخصية و حاجات من يعيلهم، وليس بهدف إعادة بيعها أو تحويلها أو استخدامها في نطاق نشاطه المهني[3].

---

[1]. شكري سرور (محمد): التجارة الالكترونية و مقتضيات حماية المستهلك، بحث مقدم إلى المؤتمر العلمي، أكاديمية شرطة دبي، الإمارات العربية المتحدة 26 – 27 فيفري، 2003، ص 176.

[2]. القانون رقم 03/09 المؤرخ في 2009/02/25 المتعلق بحماية المستهلك و قمع الغش، الصادر في الجريدة الرسمية عدد 15، بتاريخ 2009/03/08.

[3]. حجازي عبد الفتاح (بيومي): النظام القانوني لحماية التجارة الإلكترونية، الجزء 1، (دون طبعة) الإسكندرية، دار الفكر الجامعي، 2002، ص 138، أنظر أيضا:

CHDEB. R, Le régime juridique du contrat de consommation, étude comparative – droit français , droit libanais et égyptien L.G, DJ, édition Alpha, paris, 2010, p 2018.

و هناك من عرفه بأنه: "كل شخص يقوم بعمليات الاستهلاك - إبرام التصرفات - التي تمكنه من الحصول على المنتجات و الخدمات من أجل إشباع رغباته الشخصية أو العائلية"[1].

و عند علماء الاقتصاد المستهلك هو: "من يشتري سلعا أو خدمات لاستعماله الشخصي أو هو الشخص الذي يحوز ملكية السلعة" [2].

و في الجزائر كان المشرع قبل صدور قانون حماية المستهلك يدرج حماية لهذا الأخير وفقا لقواعد القانون المدني أي في إطار المسؤولية التعاقدية أو المسؤولية التقصيرية، أما بعد صدور قانون حماية المستهلك رقم 02/89 المؤرخ في 07/ 1989/02، و المتعلق بالقواعد العامة لحماية المستهلك[3] بدأت تتبلور حماية المستهلك و المبادئ الأساسية لضمان حقوقه.

و بهذا نستنتج أن مفهوم المستهلك أصبح أكثر أهمية، و من خلال هذا القانون أصبح من الواضح أن المشرع الجزائري يدرك خطورة المركز الذي أصبح يحتله المستهلك قانونيا و واقعيا في ظل التطورات الحاصلة و كذلك في ظل توجه الجزائر نحو نظام اقتصاد السوق و ما يحمله من تنوع المنتجات و كثرتها و تنوع الخدمات المعروضة، ثم جاء القانون الجديد المتعلق بحماية المستهلك و قمع الغش رقم 03/09 المؤرخ في 2009/02/25 السابق ذكره ليقوي الحماية للمستهلك وخصوصا في ظل التطورات الحاصلة.

و قد عرفه في المادة 3 منه كما يلي: "المستهلك هو كل شخص طبيعي أو معنوي يقتني بمقابل أو مجانا سلعة أو خدمة موجهة للاستعمال النهائي، من أجل تلبية حاجة شخص آخر أو حيوان متكفل به".

و يتضح أن المشرع الجزائري حاول توسيع مفهوم المستهلك الذي أصبح يطال الشخص المعنوي إلى جانب الشخص الطبيعي بغض النظر عن دفعه مقابل السلعة أو الخدمة أو لا، ولابد أن يستفيد هذا الشخص المعنوي من الحماية القانونية و بهذا التعريف نجد أن المشرع الجزائري قد أغلق باب الاجتهاد من طرف الفقه و القضاء من أجل تعريف المستهلك.

---

[1]. عبد الباسط جمعي (حسن): حماية المستهلك، الحماية الخاصة لرضا المستهلك في عقود الاستهلاك، مجلة الدراسات القانونية، العدد 13، كلية الحقوق، جامعة أسيوط، 1991، ص 247.

[2]. صياد (الصادق): حماية المستهلك في ظل القانون الجديد رقم 09-03 المتعلق بحماية المستهلك و قمع الغش، مذكرة لنيل شهادة الماجستير في العلوم القانونية و الإدارية، تخصص قانون الأعمال جامعة الإخوة منتوري، قسنطينة 1، 2013 -2014، ص 31.

[3]. القانون رقم 02/89 المؤرخ في 1989/02/07، و المتعلق بالقواعد العامة لحماية المستهلك الجريدة الرسمية، عدد 6، المؤرخة في 1989/02/08.

أما بالنسبة لتعريف المستهلك الإلكتروني فهو ذلك الشخص الذي يبرم عقودا إلكترونية مختلفة من شراء و بيع و إيجار و قرض و انتفاع و غيرها من العقود بغرض توفير ما يحتاجه من سلع و خدمات لإشباع حاجياته الشخصية و العائلية دون أن يكون الغرض من ذلك هو إعادة تسويقها و دون أن تتوفر لديه الخبرة الفنية لمعالجة هذه ا أشياء و إصلاحها[1].

مع العلم أن المشرع الجزائري و في إطار القانون 05/18 في المادة 06، قد عرف المستهلك الالكتروني بأنه: "كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الاتصالات الالكترونية من المورد الالكتروني بغرض الاستخدام النهائي"[2].

و بهذا فتعريف المستهلك الإلكتروني لا يخرج عن تعريف المستهلك التقليدي و لا يخرج عن التعريف الذي أراده المشرع الجزائري عدا في خاصية واحدة هي أن المستهلك الإلكتروني هو الشخص الطبيعي أو المعنوي الذي يقتني سلع و خدمات لإشباع حاجاته الشخصية و العائلية خارج أعمال مهنته عبر الإنترنت، و لأنه قد أصبحت فكرة المستهلك مهمة في مجالات عديدة ومنها التجارة الإلكترونية، فأصبح المستهلك الإلكتروني أمام رقعة واسعة للاختيار الحر أين أصبح للعرض و الطلب مفاهيم رقمية و بهذا أصبح المستهلك الإلكتروني في حاجة ملحة للحماية في ظل التجارة الإلكترونية فهو يتعرض لخطر أكبر و أوسع.

ثانيا: أركان جريمتي الغش و الخداع الواقعة على المستهلك الإلكتروني.

لقد نظم المشرع الجزائري جريمة الغش في المادة 431 من قانون العقوبات الجزائري، فنص على حظر مجموعة من الأفعال التي تتضمن غش المواد الاستهلاكية الصالحة لتغذية الإنسان أو الحيوان أو مواد طبية أو فلاحيه مخصصة للاستهلاك بما يتناسب مع مضمون المادة 70 من القانون رقم 03/09[3] المتعلق بحماية المستهلك و قمع الغش التي استعمل فيها المشرع لفظ "التزوير" من أجل التعبير عن الغش[4].

---

[1]. جبلو (جميلة): حماية المستهلك في العقود الإلكترونية، مجلة الاقتصاد الجديد، المجلد 1، العدد 10، الجزائر، خميس مليانة، 2014، ص 6211.

[2]. القانون 05/18 المتعلق بالتجارة الالكترونية، المؤرخ في 2018/05/10، و الصادر في الجريدة الرسمية عدد 28، بتاريخ 2018/05/16.

[3]. أنظر... القانون القانون رقم 09-03 المؤرخ في 2009/02/25 المتعلق بحماية المستهلك و قمع الغش السابق ذكره.

[4]. أنظر ... أكسوم عيلام (رشيدة) : مرجع سابق، ص392.

أما الخداع فلم يقدم له هذا الأخير تعريفا في التشريع العقابي و اكتفى في نص الماد 429 من قانون العقوبات بتعداد طرق و وسائل خداع المتعاقد بصفة عامة حيث تشكل الأفعال الإيجابية المكونة لجريمة الغش خداعا للمستهلك أين عدد المجالات التي يمكن أن تنصب عليها جريمة الخداع[1].

1: الركن المادي لجريمتي الغش و الخداع الواقعتين على المستهلك الإلكتروني.

قد يكون الإنسان ضحية لبعض الجرائم كالفساد أو بيع مواد مغشوشة فالركن المادي هنا هو أي فعل أو سلوك محظور صادر من الإنسان يمكن أن يسبب ضررا و يجب أن تكون علاقة سببية بين الفعل و النتيجة ، و هنا يتشكل الركن المادي للجريمة الإلكترونية كالشخص الذي يشتري برامج الاختراق لاستعمالها في سرقة رقم البطاقة الأئتمانية عبر الإنترنت و الركن يمكن أن يتوفر في حالة البيع الإلكتروني كغش التاجر في عرضه لسلع غير صالحة للاستهلاك.

و بهذا فقد يطرأ الغش على مواد صالحة لتغذية الإنسان أو الحيوان أو المواد الطبية أو المنتجات الفلاحية و يمكن أن يكمن الغش في عرض أو بيعها مع العلم بأنها مغشوشة كما يمكن أن ينصب الغش على التعامل بمواد خاصة تستعمل من أجل تغشيش المواد أو لمجرد الحث و التحريض على استعمال هذه المواد بواسطة كتيبات أو منشورات أو إعلانات مهما كانت طبيعتها[2].

أين استعمل لفظ التزوير بدل الغش و أحال في تقرير العقوبات بشأنها لأحكام قانون العقوبات لكنه وسع في دائرة المنتج محل الغش ، و يعتبر هذا الأخير من قبيل الأفعال التي تؤدي إلى قيام المحترف بمخالفة إلزامية أمن المنتج الذي يتدخل في عملية عرضه للاستهلاك و ذلك وفقا لحكم المادة 83 من القانون 03/09 السابق ذكره، و قد حددت المادة 10 منه التزامات المحترف في توفير أمن المنتجات فيما يخص مميزات و تركيب و تغليف و شروط تجميع و صيانة المنتج ووسم المنتوج و إرفاقه بالتعليمات الخاصة باستعماله و إتلافه، و كل الإرشادات و المعلومات الصادرة عن المحترف خاصة فيما يتعلق بتأثير المنتوج على المنتوجات الأخرى عند توقع استعماله مع هذه المنتوجات و تحديد الفئات المعرضة للأخطار من استعمال المنتوج[3].

---

[1]. المرجع نفسه، ص392.

[2]. أنظر ... المادة 431 من قانون العقوبات الجزائري، و المادة 70 من القانون رقم 03/09 المتعلق بحماية المستهلك و قمع الغش السابق ذكرهما.

[3]. أكسوم عيلام (رشيدة) : مرجع سابق، ص402.

أما بالنسبة للركن المادي لجريمة خداع المستهلك الإلكتروني، المتعاقد عبر الانترنت فتتحقق بخداع أو محاولة خداع هذا الأخير في البيانات المتعلقة بالسلعة كطبيعة أو في الصفات الجوهرية في تركيب و نوع و مصدر أو كمية السلعة، و قد وسع المشرع الجزائري من حماية المستهلك عموما وفقا لنص المادة 68 من القانون رقم 03/09 المتعلق بحماية المستهلك و قمع الغش السابق ذكره، فلا تقتصر واقعة الخداع على السلع و إنما على المنتوج بصفة عامة أي كل من السلع و الخدمات فيتم ارتكاب جريمة الخداع بواسطة الوزن أو الكيل أو بأدوات أخرى مزورة أو غير مطابقة للمواصفات أو من خلال استعمال وسائل ترمي إلى التغليط في عمليات التحليل أو المقدار أو الوزن أو الكيل أو التغيير عن طريق الغش في تركيب أو وزن أو حجم المنتوج الذي يتم عرضه إلكترونيا عبر الإنترنت[1].

2: الركن المعنوي لجريمتي الغش و الخداع الواقعتين على المستهلك الإلكتروني.

يتمثل الركن المعنوي في جريمة الغش في توفر القصد الجنائي أي اتجاه إرادة الجاني إلى ارتكاب فعل ضد حق يحميه القانون و يعاقب عليه و القيام بعمل غير مشروع، و هنا نجد أن المحترف المتدخل في عملية عرض المنتج للاستهلاك بما ينطوي عليه سلوكه من غش في السلعة أو ما يتعامل به من خلال أداء نشاطه المهني بنية غش المستهلك أما عن وقت العلم بالغش فيستوي أن يعلم به المحترف عند بداية العرض للمنتوج أو في وقت لاحق و تخضع هذه المسألة للسلطة التقديرية للقاضي، مع الأخذ بعين الاعتبار دور المحترف في عملية عرض المنتوج للاستهلاك إذ يعتبر الصانع و المنتج و الحرفي أول المتدخلين في عملية عرض المنتوج للاستهلاك، لتتوالى عدة فئات أخرى من الأشخاص المحترفين من أجل إيصال المنتوج للمستهلك كالمستورد و الوسيط والناقل و تاجر الجملة و تاجر التجزئة فإثبات القصد و توفر العلم في المنتج و الصانع يتباين عن قصد البائع و مدى توفر علمه بكون المنتوج مغشوشا[2].

كما أن قيام جريمة خداع المستهلك الإلكتروني يرتبط بتحقق القصد الجنائي للمحترف المتدخل في عملية عرض المنتوج للاستهلاك الساعي لخداع المستهلك و ذلك من خلال العلم و انصراف

---

[1]. أكسوم عيلام (رشيدة) : مرجع سابق، ص 403.

[2]. أنظر ... بن براهيم بن علي الحوشاني(فهد): الغش في المعاملات التجارية الالكترونية بين الفقه و النظام السعودي، رسالة ماجستير، الجامعة الأردنية، كلية الدراسات العليا، 2006، ص 94 و ما والاها.

إرادته إلى الإتيان بواقعة التعدي مستعينا في ذلك بالوسائل الإلكترونية فالركن المعنوي يتمثل في علاقة نفسية بين السلوك الإجرامي و نتائجه بين الفاعل الذي يأتي هذا السلوك[1].

المحور الثاني: إجراءات حماية المستهلك الإلكتروني من جريمتي الغش و الخداع و العقوبات المرصودة.

تعتبر الحماية الجزائية أعلى درجات الحماية للفرد و المجتمع و إن كان قد سبق حماية المستهلك التقليدي من غش و خداع المحترف فإن هذه الحماية لها من الخصوصية لطبيعة الأرضية التي يلتقي فيها المحترف بالمستهلك الإلكتروني و إن كانت القواعد الحمائية العامة هي ذاتها إلا أنه هناك ما يميز حماية المستهلك الإلكتروني سواء من الناحية الإجرائية أو العقابية.

أولا: الإجراءات الجزائية المتبعة لمواجهة الغش و الخداع الواقع على المستهلك الإلكتروني.

يقتضي النظام الإجرائي عموما و الذي هو بصدد المعاينة و التحقيق في وقوع الجرائم أن تسند هذه المهام لمن هو مخول لها قانونا، و وفقا للإجراءات القانونية المنصوص عليها في قانون الإجراءات الجزائية الجزائري أو في القوانين الخاصة، و هذا تحت طائلة تعرض هذه الإجراءات للبطلان نتيجة حساسيتها و إمكانية المساس بخصوصيات الأشخاص سواء كانوا طبيعيين أو معنويين، و في إطار المحافظة على الشرعية الإجرائية المحمية دستوريا.

1: الأشخاص المكلفون بحماية المستهلك الإلكتروني من الغش و الخداع.

يمكن الإشارة إلى أن قانون الإجراءات الجزائية الجزائري قد أسند مهمة التحري عن هذا النوع من الجرائم كاختصاص عام لضباط الشرطة القضائية، الذي لهم صفة الضبطية حسب ما تنص عليه المادة 15 من هذا الأخير، و هم على تعدادهم : رؤساء المجالس الشعبية البلدية و ضباط الدرك الوطني و ذوو الرتب في الدرك و رجال الدرك الذين لهم أقدمية ثلاث سنوات على الأقل في سلك الدرك و الذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل و وزير الدفاع و مفتشوا الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل و عينوا بموجب قرار مشترك صادر عن وزير العدل و وزير الداخلية و الجماعات المحلية و ضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك بين وزير الدفاع الوطني و وزير العدل[2].

---

[1]. أكسوم عيلام (رشيدة) : المرجع نفسه، ص398.

[2].أنظر ... المواد 15 و ما والاها من قانون الإجراءات الجزائية الجزائري المعدل بالأمر رقم 02/15 المؤرخ في 23 جويلية، و الصادر في الجريدة الرسمية رقم 40 بتاريخ 23/جويلية 2015.

كما أن المشرع الجزائري قد رخص لأعوان بموجب نصوص خاصة إجراء التحري عن هذا النوع من الجرائم، و منهم الوالي الذي يعتبر ممثلا للدولة على مستوى الولاية التي يشرف عليها وتخضع لسلطته المديريات الولائية للتجارة و التي تسهر على ممارسة القواعد التجارية، و قواعد المنافسة و كذلك قواعد حماية المستهلك، هذا الأخير الذي يقوم باتخاذ الإجراءات اللازمة في الإطار القانوني للدفاع عن مصالح فئة المستهلكين عموما و ذلك بإشرافه على مديرية التجارة، وتسخر له قوة عمومية تمكنه من تجسيد و فرض قراراته[1].

كما أنه هناك أعوان قمع الغش و هم نوع من الموظفين الذين تسند لهم مهام لقمع الغش و هم تابعين لوزارة التجارة، و هم إلى جانب أعوان المنافسة و التحقيقات الاقتصادية، يلتزمون بأداء اليمين أمام محكمة مقر إقامتهم الإدارية التي تسلم إشهادا بذلك و لهم عند الاقتضاء القيام بجملة من الإجراءات و منها الإجراءات التحفظية المنصوص عليها في مجال قمع الغش ، و في هذا الإطار هناك ثلاث أسلاك منهم، و هم سلك مراقبي الغش و سلك محققي قمع الغش و سلك مفتشي قمع الغش[2].

2: السبل المتبعة لمنع الغش و الخداع الواقع على المستهلك الالكتروني.

إن المحترف الإلكتروني يخضع لنفس الإجراءات التي يخضع لها المحترف التقليدي حسب نص المادة 53 من القانون رقم 03/09، المتعلق بحماية المستهلك و قمع الغش السابق ذكره، ولو أن هذا الأخير له بعض الإجراءات الخاصة تبعا، للفضاء الذي يتم فيه التعامل غير المشروع.

و من الإجراءات التقليدية نجد رفض دخول المنتجات المستوردة، حسب نص المواد 53 و54 من القانون 03/09 السابق ذكره، و ذلك من طرف الأعوان المكلفين قانونا بذلك، حيث لهم الرفض المؤقت للمنتوج في حالة الشك و عدم المطابقة فيوقف عند الحدود لإجراء التحريات اللازمة، و في حالة ثبوت المخالفة يتم التصريح بالرفض النهائي.

كما لهم القيام بإجراء الإيداع المتعلق بالمنتوج، حسب نص المواد من 55 إلى 58 من القانون السابق، و ذلك من أجل ضبط المطابقة و اعذار المحترف بضرورة اتخاذ التدابير اللازمة لمعالجة سبب عدم المطابقة، أو إزالتها، و في حالة تعذر ذلك يتقرر حجز المنتوج.

---

[1]. أنظر ...مجدوب (نوال): حماية المستهلك جنائيا من جريمة الخداع في عملية تسويق المواد الغذائية، مجلة دفاتر السياسة و القانون، العدد 15، جوان 2016، ص 270.

[2]. أنظر... أكسوم عيلام (رشيدة) : مرجع سابق، ص400.

كما أنه هناك إجراء سحب المنتوج حسب المواد 59 إلى 63 من القانون 03/09 السابق ذكره، أين يمنع تداول المنتوج بعد إجراء التحاليل اللازمة و إن تم ثبوت مطابقة المنتوج يرفع إجراء السحب، مع تعويض المحترف عما وقع عليه من ضرر و لو أن المادة 62 من القانون السابق قد أعطت الصلاحية الكاملة لهؤلاء الأعوان من أجل سحب المنتوج نهائيا دون الحصول على رخصة من السلطة القضائية في حالة ثبوت أن المنتوجات موضوع الشك تأكد أنها مزورة أو مغشوشة أو سامة أو انتهت مدة صلاحيتها أو عدم صلاحيتها أصلا للاستهلاك و كذا المنتوجات التي تستعمل في التزوير و المنتوجات المقلدة، مع تحرير محاضر بذلك و تشميع المنتوجات و وضعها تحت الحراسة أو سحبها مؤقتا أو نهائيا إن كان لازم إتلاف هذه الأخيرة و هذا حسب نص المادة 64 من القانون 03/09 السابق ذكره.

كما يمكن أن يتم توقيف نشاط المحترف بعد ثبوت عدم احترامه لما ينص عليه القانون، ويتحمل المحترف المقصر المصاريف عن الإجراءات التحفظية، بما في ذلك مصاريف إجراء الإيداع وإعادة المطابقة و السحب المؤقت، و تغيير الاتجاه و إعادة التوجيه و الإتلاف وتحمل مصاريف استرجاع المنتوج المشتبه فيه أينما وجد و كذا المصاريف المقررة في حالة السحب النهائي للمنتوج.

و هناك آليات مستحدثة في ظل مشروع قانون التجارة الإلكتروني منها غلق الموقع لإلكتروني للمحترف بموجب أمر من القاضي و ذلك لمدة تتراوح ما بين شهر إلى ستة أشهر، و ذلك من خلال التعامل في مجموعة من المنتوجات عن طريق الاتصالات الالكترونية و التي تم تحديدها في المواد 3 و 4 من مشروع قانون التجارة الالكترونية، كما يمكن للقاضي أن يأمر بشطب المحترف الالكتروني من السجل التجاري، في حالة قيام هذا الأخير بالتعامل في أجهزة و عتاد حساس يخضع لتنظيم خاص و كذا التعامل بمنتوجات من شأنها المساس بالأمن و النظام العام، و أيضا تعليق النفاذ إلى منصات الدفع الإلكتروني نتيجة مخالفة المحترف الإلكتروني لالتزامه بتقديم إعلان نزيه...، كما يتعرض المحترف الإلكتروني إلى تعليق تسجيل أسماء النطاق عند عدم القيام بإجراءات التسجيل الضرورية في السجل التجاري مسبقا.[1]

ثانيا: العقوبات المرصودة لحماية المستهلك الإلكتروني من جريمتي الغش و الخداع.

إن المحترف الذي قد يقوم بخداع المستهلك الالكتروني ليس بالضرورة أن يكون شخصا طبيعيا بل قد يكون شخصا معنويا أيضا و لهذا لا بد من إفراد عقوبة لكليهما حسب خصوصية كل واحد منهما.

---

[1]. أنظر... أكسوم عيلام (رشيدة) : مرجع سابق، ص408 و ما والاها.

1: العقوبات المرصودة للمحترف كشخص طبيعي الذي يثبت غشه و خداعه.

تتباين عقوبة المحترف كشخص طبيعي بحسب درجة جسامة الضرر الذي يحدثه بفعل واقعة الغش و الخداع إلا أن مجرد الشروع في الجريمة أو قيامها مع عدم ترتيب أضرار لا يعفي المحترف من العقوبات الجزائية التي تمثل في الحبس لمدة تتراوح بين شهرين إلى خمس سنوات و غرامة ما بين ألفين إلى خمس مائة ألف دينار جزائري، و تشدد هذه العقوبات إذا أفضت هذه المنتوجات إلى مرض أو عجز عن العمل للمستهلك الإلكتروني بالحبس من خمس إلى عشر سنوات و بغرامة من خمس مائة ألف إلى مليون دينار جزائري، و تضاعف العقوبة بالحبس من عشر سنوات إلى عشرين سنة و الغرامة إلى مليونين إذا تسبب خداع و غش المستهلك في مرض غير قابل للشفاء أو فقد استعمال عنصر أو الإصابة بعاهة مستديمة[1].

2: العقوبات المرصودة للمحترف كشخص معنوي الذي يثبت غشه و خداعه.

حسب ما تنص عليه المادة 51 مكرر من قانون العقوبات الجزائري[2] فإن الشخص المعنوي المحترف حسب المادة 51 المحال إليها من المادة الأولى و الذي يخضع للقانون الخاص يكون مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك، و منها ما يرتكب من جرائم الغش و الخداع مع إمكانية مساءلة الشخص الطبيعي الممثل له كفاعل أصلي أو كشريك و يوقع عليه عقوبات حب نص المادة 18 مكرر إلى 18 مكرر 2 من قانون العقوبات الجزائري[3] و من العقوبات الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي ... بالإضافة إلى إمكانية فرض عقوبات تكميلية و المتمثلة في حل الشخص المعنوي و غلق المؤسسة و الإقصاء من الصفقات العمومية و المنع من مزاولة نشاط أو عدة أنشطة مهنية و مصادرة الشيء و نشر و تعليق حكم الإدانة مع الوضع تحت الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته، كما أن المشرع الجزائري نص على إجراء غرامة الصلح كإجراء بديل.

---

[1]. أنظر ... المواد 429 و 430 من قانون العقوبات السابق ذكره، و المادة 435 من نفس القانون، أنظر أيضا... أكسوم عيلام (رشيدة): مرجع سابق، ص 410 و 411، و ...بودالي (محمد): شرح جرائم الغش في بيع السلع و التدليس في المواد الغذائية و الطبية، الجزائر ديوان المطبوعات الجامعية،2006 ، ص 13 و ما والاها.

[2]. أنظر .. المواد 51 مكرر من قانون العقوبات الجزائري المعدل بالقانون رقم 91/15 المؤرخ في 2015/12/30 و الصادر في الجريدة الرسمية رقم 71 بتاريخ 2015/12/30.

[3]. أنظر ... المواد 18 مكرر و ما والاها من نفس القانون.

و قد تم تحديد العقوبات المطبقة على المحترف وفقا لما تنص عليه المواد من 68 إلى 85 من القانون رقم 03/09 المتعلق بحماية المستهلك و قمع الغش، الذي أحالنا على نصوص قانون العقوبات في مواده 429 و 431 و 432 و 435 و قد فرض المشرع عقوبة السجن المؤبد حسب المادة 3/83 من القانون 03/09 على المحترف المخالف الذي يتسبب في وفاة شخص أو أكثر، أما العقوبات المالية المطبقة عليه فهي حسب القانون الأخير الغرامة ما بين خمسون ألفا إلى مليون دينار جزائري، و هذا حسب نوع الالتزام، كما نص المشرع على إمكانية إجراء دفع غرامة الصلح حيث تفرض من طرف أعوان قمع الغش على المحترف و في حالة المخالفة تطبق عليه عقوبات مالية، و تحدد غرامة الصلح حسب نوع واقعة المخالفة و تتراوح ما بين خمسين ألفا إلى ثلاث مائة ألف دينار جزائري، أو فرض نسبة عشرة في المائة من ثمن بيع المنتوج في حالة رفض تنفيذ خدمة ما بعد البيع و في تسجيل عدة مخالفات في نفس المحضر فيلزم المحترف المخالف بدفع مبلغ إجمالي لكل غرامات الصلح المستحقة [1].

خاتمة.

إن جريمتي الغش و الخداع الواقعتين على المستهلك الإلكتروني تعدان أحد أخطر الجرائم الواقعة على هذا الأخير في الفضاء الرقمي، فالمحترف الالكتروني و هو المتدخل في عملية التسويق بشتى مراحلها يكون قد خان و خرق صفة الائتمان كدعامة أساسية في التجارة الإلكترونية.

و عند النظر للمنظومة العقابية التي تجرم هذه الأفعال العامة منها و المتخصصة نجد عدة ثغرات تشريعية صارخة و متجسدة بالأساس في نطاق جنحة الغش و الخداع من حيث الأشخاص والتي تنصب على المستهلك بموجب قانون الاستهلاك و منه المستهلك الإلكتروني و على المتعاقد (الإلكتروني) من خلال قانون العقوبات.

و كذا نجد أن المشرع يستعمل تارة لفظ سلعة بموجب أحكام قانون العقوبات و تارة لفظ المنتوج بموجب قانون الاستهلاك و هذا اللفظ أوسع من الأول و نحن في ظل عدم اللجوء إلى تفسير النص الجنائي فكيف سوف يقرن النص الخاص و يقيد العام و خصوصا إذا كان الخاص يحيل على العام في كثير من الأحيان خصوصا و أن لفظ المنتوج يتضمن كل من السلعة والخدمة.

---

[1]. أنظر... سعداوي (سليم): عقود التجارة الالكترونية، دراسة مقارنة، (دون طبعة)، الجزائر، دار الخلدونية، 2008، ص 28 و ما والاها.

لهذا كان لابد من التنسيق بين النصين العام و الخاص و خصوصا إذا كانت الغاية هي حماية المستهلك عموما و منه المستهلك الإلكترون.

و هناك أيضا قلة التخصص في خبايا التطور التكنولوجي للقائمين على الرقابة الإلكترونية في التعاملات التجارية و هو الأمر الذي يجب أن يتوفر تدعيما للحماية المرجو توفيرها للمستهلك الإلكتروني.

بيع المواد الصيدلانية على شبكة الانترنيت و المسؤولية الجنائية المترتبة عنها

The sale of pharmaceuticals on the Internet and the criminal liability for it

د. المر سهام أستاذة محاضرة أ

معهد الحقوق و العلوم السياسية

المركز الجامعي بمغنية - الجزائر

مقدمة:

يشكّل البيع على شبكة الإنترنيت في عصر العولمة حصة الأسد، فقد امتد نطاق هذه العولمة إلى غاية المواد الصيدلانية، حيث تمتع هذه الأخيرة، وخاصة الدواء بنوع من الخصوصية المستمدة من أنّ حاجة الإنسان إليها لا تتوقف، فهي ترتبط مباشرة بحياة الإنسان وسلامته الجسدية، ولهذا اكتسبت هذه الأهمية الحيوية خاصة في ظل الحياة المعاصرة وما ترتب عنها من تطورات ومفرزات سلبية على صحة الإنسان وقدرته المعيشية[1]، فهذه المكانة التي تربع بها الدواء خاصة و المواد الصيدلانية عامة على قائمة السلع الضرورية، كانت نتيجة أهمية الدور الذي يمثله بالنسبة للإنسان، ومن كونها تهدف إلى تحقيق الشفاء الكامل له أو على الأقل تخفيف الآلام التي يعاني منها، فإذا كان باستطاعة الإنسان أن يستغني عن المنتجات الاستهلاكية الأخرى باختلاف أنواعها، فهو في أمس الحاجة إلى دواء يكفي حاجته في العلاج.[2]

---

[1] أعلنت المديرة العامة لمنظمة الصحة العالمية الدكتورة "مارغريت نشان" في الاجتماع الوزاري المتعلق بالتغطية الصحية الشاملة بأن الفواتير الطبية المرتفعة الباهظة، تدفع ما يتراوح بين 100 و150 مليون شخص تحت خط الفقر كل عام وهذا بالرغم من أنّ العديد من الحكومات تسعى جاهدة إلى انتشال الناس من هوية الفقر. (كلمتها الملقاة في سنغافورة 10 فبراير 2015).

www.who:int/dg/speeches/2015/singaporeuhc/ar/-49k

[2] جمال عبد الرحمن محمد علي، المسؤولية المدنية لمنتجي المستحضرات الصيدلانية، رسالته دكتوراه في الحقوق، كلية الحقوق جامعة القاهرة، سنة 1993، ص.201.

فاجتماع أبعاد علمية وتكنولوجية وتاريخية واقتصادية وأخلاقية ومستقبلية في سلعة واحدة هو أمر غير عادي، وإذا كانت هذه الأبعاد تجتمع بوضوح في المواد الصيدلانية، فلا ريب أنه يصبح محلا لإشكاليات وتحديات محلية وعالمية.[1]

كل هذا جعل من المواد الصيدلانية منتوجات حيوية ترتبط ارتباطا وثيقا بالصحة البشرية والحيوانية، لا ينبغي التعامل معها على أنها منتجات تجارية، بل يجب توخي كل الحذر والحرص عند التعامل معها لما لها من أبعاد إنسانية واجتماعية خطيرة. فالمواد الصيدلانية أصبحت من أهم متطلبات حياة الإنسان وحياة الحيوان الذي قد يكون محل استثمار اقتصادي تجاري، أو كائن أليف صديق في البيئة، تتطلب المحافظة على الصحة العامة حمايته من الأمراض والأوبئة.[2]

و عليه و أمام إمكانية بيع المواد الصيدلانية عبر شبكة الانترنيت، فما هو موقف المشرع الجزائري من هذه المسألة، و هل أجاز عملية بيعها عبر شبكة الانترنيت، و في حالة إقصائها من نطاق التجارة الإلكترونية، فكيف تقوم المسؤولية الجنائية المترتبة عنها؟

و للإجابة عن هذه الإشكالية ارتأينا تقسيم الموضوع إلى مبحثين نتناول في المبحث الأول بيع المواد الصيدلانية عبر شبكة الانترنيت، في حين نخصص المبحث الثاني للمسؤولية الجنائية لبائع المواد الصيدلانية عبر شبكة الانترنيت.

المبحث الأول: بيع المواد الصيدلانية على شبكة الانترنيت

لقد بات بيع المواد الصيدلانية حقيقة لابد أن يكون لها تأطير قانوني خاص بها، و هذا ما سنحاول أن نبينه في هذا المبحث ، حيث سنستهله بتحديد مفهوم المواد الصيدلانية و بائعيه كمطلب أول، كما سنتناول في المطلب الثاني التأطير القانوني لعملية البيع عبر شبكة الانترنيت مبرزين موقف المشرع الجزائري.

المطلب الأول: مفهوم المواد الصيدلانية و بائعها.

سنحاول في هذا المطلب الوقوف عند مفهوم المواد الصيدلانية و كذا بائعيها .

الفرع الأول: مفهوم المواد الصيدلانية

[1] نصر أبو الفتوح فريد حسن، حماية حقوق الملكية الفكرية في الصناعات الدوائية، دراسة مقارنة، دار الجامعة الجديدة، سنة 2007، ص.87.

[2] جنون البقر، أنفلونزا الخنازير، الطيور.

لقد تناول المشرع المواد الصيدلانية في إطار الباب الخامس من قانون الصحة، الصادر بموجب القانون رقم 18-11 المؤرخ في 02 يوليو 2018 الملغي لأحكام القانون 85-05 المؤرخ في16 فبراير سنة 1985،[1] تحت عنوان: "المواد الصيدلانية والمستلزمات الطبية"، حيث نصت المادة 207 منه على تحديد المواد الصيدلانية بأنها: "تتضمن المواد الصيدلانية في مفهوم هذا القانون، ما يأتي:

- الأدوية،
- الكواشف البيولوجية،
- المواد الكيميائية الخاصة بالصيدليات،
- المواد الجالينوسية،
- المواد الأولية ذات الاستعمال الصيدلاني،
- الأغدية الحميوية الموجهة لأغراض طبية خاصة،
- كل المواد الأخرى الضرورية للطب البشري."

ما يلاحظ من خلال المادة 207 من ق.ص.[2] أن المشرع لم يعط تعريفا دقيقا للمواد الصيدلانية، وإنما انتهج طريقة التعداد للمواد التي تدخل في نطاقها ، حيث يبدو من الوهلة الأولى أن التعداد الوارد جاء على سبيل الحصر لا على سبيل المثال، غير أن الفقرة الأخيرة من نفس المادة "كل المواد الأخرى الضرورية للطب البشري" غيرت الاتجاه.

لقد استهل المشرع المواد الصيدلانية بالدواء، الذي نجده في مقدمة مجموعة المواد التي تدخل في نطاق المواد الصيدلانية، كونه المصدر والأساس التقليدي في العلاج، حيث لا يمكن إنكار الحاجة الملحة إليه حالة تقرير داء، وكذلك نظرا لشيوع استهلاكه واستعماله بين كافة الناس،

[1] القانون رقم 85-05 المؤرخ في 26 جمادى الأولى عام 1405 الموافق لـ 16 فبراير سنة 1985 والمتعلق بحماية الصحة وترقيتها، المعدل والمتمم بموجب القانون رقم 08-13 المؤرخ في 17 رجب عام 1420 الموافق لـ 20 يوليو سنة 2008، ج.ر.ع. 44 المؤرخة في 03 غشت سنة 2008 الملغى بمقتضى القانون رقم 18-11، المؤرخ في 02 يوليو سنة 2018، المتعلق بالصحة، الصادر في ج.ر.ع. 46 المؤرّخة في 29 يوليو 2018.

[2] القانون رقم 18-11 المتعلق بالصحة، المشار إليه سابقا.

ولأهميته فقد خصه المشرع بمادتين من ق.ص. وهما المادة 208 والتي جاء فيها بمفهوم الدواء، وكذلك المادة 209 التي تحدث فيها عن المنتجات المماثلة للأدوية.

حيث جاء في المادة 208 من ق.ص. ما يلي: "الدواء في مفهوم هذا القانون هو كل مادة أو تركيب يعرض على أنه يحتوي على خاصيات علاجية أو وقائية من الأمراض البشرية أو الحيوانية وكل المواد التي يمكن وصفها للإنسان أو للحيوان قصد القيام بتشخيص طبي أو استعادة وظائفه الفيزيولوجية أو تصحيحها وتعديلها،

وعليه فقد حاول المشرع من خلال المادة 208 من ق.ص.[1] إيراد تعريف دقيق للدواء لإزالة كل لبس وشك حيث اعتمد في تحديده للمقصود بالدواء على أسلوبين أو طريقتين:

- طريقة التعريف الجامع الشامل: وتظهر من خلال الفقرة الأولى من المادة **208** من **ق.ص.** والتي نصت على ما يلي "كل مادة أو تركيب يعرض على أنه يحتوي على خاصيات علاجية أو وقائية..."

- طريقة التعريف المصنف والمحدد: وتظهر من خلال المادة **210** من **ق. ص** حيث نلاحظ أن المشرع قد حاول حصر وضبط كل المواد المستحدثة في مجال الصحة، ليضعها ضمن تصنيف خاص بها.

الفرع الثاني: مفهوم بائع المواد الصيدلانية

إنّ بائع المواد الصيدلانية هو ذلك الصيدلي الذي يقوم بمهمة تحضير وصرف الأدوية بناء على وصفة طبية، حيث أنّ المريض لا يمكن أن يتحصل على الدواء مباشرة من المنتج، بل يتوسط بينه وبين المنتج عدة وسطاء منهم الصيدلي البائع، إلاّ إذا تعلّق الأمر بالمستحضر الوصفي وكذلك المستحضر الاستشفائي والمستحضر الصيدلي، والمحضر في الصيدلية تنفيذا لوصفة طبية والمقدّم مباشرة للمريض.

فبائع المستحضرات الصيدلانية من الناحية القانونية هو من يحتكر عملية البيع، والذي قد يكون إمّا الصيدلي بوصفه المسؤول عن الصيدلية أو مساعد الصيدلي أو الطبيب البيطري إذا تعلّق الأمر بالمواد الصيدلانية البيطرية.

---
[1] القانون رقم 18-11 المتعلق بالصحة، المشار إليه سابقا.

الصيدلي بوصفه مسؤولا عن الصيدلية وعن مهنة الصيدلة فإنه يتولى مهمة التوزيع بالتجزئة (البيع بالتجزئة) للمواد الصيدلانية والتي تمثل النشاط الرئيسي استنادا لنص المادة 249 من ق.ص.[1] والتي نصت على أن يتولى التوزيع بالتجزئة للمواد الصيدلانية المستعملة في الطب البشري صيدليات توضع تحت مسؤولية صيدلي، يجب أن يكون الصيدلي هو المالك الوحيد والمسيّر الوحيد للمحل التجاري للصيدلية فيما يخصّ الصيدليات الخاصة، كما يجب أن يمثل النشاط الرئيسي للصيدليات في توزيع المواد الصيدلانية المستعملة في الطب البشري، ويمكنها وبشكل ثانوي القيام بتوزيع المواد شبه الصيدلانية.

المطلب الثاني: التأطير القانوني لعملية بيع المواد الصيدلانية عبر شبكة الانترنيت

لم ينظم المشرع الجزائري بيع الأدوية على شبكة الإنترنيت، وهذا على غرار المشرع الفرنسي الذي له دور سبق الركب في مواكبة المستجدات، و ذلك من خلال تنظيم عملية بيع المواد الصيدلانية عبر شبكة الانترنيت (الفرع الأول) إضافة إلى إخضاعها للاحتكار الصيدلاني (الفرع الثاني).

الفرع الأول: تنظيم عملية بيع المواد الصيدلانية عبر شبكة الانترنيت

في فرنسا سبق القضاء التشريع في إخضاعه بيع الدواء عبر شبكة الانترنيت للاحتكار الصيدلاني، حيث عوقب كل من يمارس الصيدلة بطريقة غير مشروعة، وكذلك كل من يبيع الدواء عبر موقع غير صيدلاني، ومنها الحكم الصادر عن محكمة باريس في 14 مارس 2006، والذي أدان الممارسة غير المشروعة لمهنة الصيدلة من طرف طبيب عام مقيم بباريس، حيث كان يستعمل موقعه الإلكتروني على شبكة الانترنيت ليعرض للبيع أدوية غير مرخص بها في فرنسا مع إمكانية الحصول عليها عن طريق وصل طلب.[2]

وأمام انتشار الأدوية المزورة التي بات يروج لها عبر شبكة الانترنيت، فإن هذه الأدوية باتت تمس الملايين من المستهلكين عبر العالم، دون خضوعها لأي مراقبة حول نوعيتها وأصلها،

---

[1] -القانون رقم 18-11، المتعلق بالصحة، المشار إليه سابقا.

[2] T. Correc.de Paris, 14 mars 2006, Nouv. pharm., juil.2006, n°391, pp.78-91, cité par : Hervé DION, Droit pharmaceutique (Officine- Industrie- Pharmacies vétérinaire et des établissements de santé), édition Gualino lextenso, Paris, 2008, p.63.

فهذا النوع من التوزيع يعتبر خطيرا على الصحة العامة، خاصة مع تفشي البيع غير المشروع للأدوية في فرنسا، والذي بات يشكل انتهاكا صارخا لقواعد الاحتكار الصيدلاني.[1]

وعلى هذا تدخّل مشرّع الاتحاد الأوربي بإصدار التوجيه رقم UE/62/2011 للبرلمان الأوربي والمجلس، والمعدل للتوجيه رقم CE/83/2001 الذي أسس قانون اتحاد أوربي متعلق بالأدوية ذات الاستعمال البشري، فيما يخص منع إدخال الأدوية المزورة في سلسلة العرض القانوني للمنتجات الطبية[2] والذي أطّر البيع عبر شبكة الانترنيت للأدوية، ليسايره في ذلك المشرع الفرنسي بمقتضى الأمر رقم 2012-1427 المؤرخ في 19 ديسمبر 2012 والمتعلق بتعزيز أمن سلسلة توريد الأدوية والإشراف على بيع الأدوية عبر شبكة الأنترنيت ومكافحة تزوير الأدوية[3]، ليكمل هذا الأمر بالمرسوم رقم 2012-1562 المؤرخ في 31 ديسمبر 2012 والمتعلق بتعزيز أمن وسلامة سلسلة توريد الأدوية والإشراف على عملية بيع الأدوية عبر شبكة الانترنيت.[4]ليصدر وزير الصحة قرارا في 20 جويلية 2013 يتعلق بالممارسة الحسنة لصرف الأدوية عن طريق الانترنيت.[5] حيث أن الصيدلي سواء بوصفه شخص طبيعي أو معنوي يمكن أن يبيع عبر موقع

---

[1] Hélène GAUMANT PRAT ,Directive 2011/62/UE « Médicaments falsifiés » : Les avancées dans la lutte contre les faux médicaments, R.G.D.M, panorama de droit pharmaceutique 2014, les études hospitalières, Janvier 2015, n°2, p.122.

[2] Dir. 2011/62/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 8 juin 2011 modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain, en ce qui concerne la prévention de l'introduction dans la chaîne d'approvisionnement légale de médicaments falsifiés, JOUE L.174/74 DE 01/07/2011.

ec.europa.eu/health/files/eudralex/vol-1/...2011_62/dir_2011_62_fr.pdf

[3] - Ord. n°2012-1427 du 19 Décembre 2012 relative au renforcement de la sécurité de la chaine d'approvisionnement des médicaments, à l'encadrement de la vente de médicaments sur internet et à la lutte contre la falsification de médicaments. JORF n°0297 du 21 Décembre. p.20182

[4] - Décret n°2012-1562 du 31 Décembre 2012 relatif au renforcement de la sécurité de la chaine d'approvisionnement des médicaments, à l'encadrement vente de médicaments sur internet JORF n° 0001 du 01 janvier 2013.

[5] - Arrêté du 20 Juin 2013 relatif aux bonnes pratiques de dispensation des médicaments par voie électroniques JORF n°0144 DU 23 Juin 2013.

على شبكة الإنترنيت مرتبط بالصيدلية أدوية للاستعمال البشري دون وصفة طبية، بناء على ترخيص إداري حيث يكون الصيدلي مسؤولا عن كل ما يحتويه موقعه الإلكتروني.[1]

في فرنسا هذه الطريقة الجديدة لصرف الدواء منظمة بمقتضى المواد من L.5125-33 إلى المادة L.5125-41 من ق.ص.ع.ف، وكذلك المواد من R.5121-70 إلى المادة R.5125-74 من ق.ص.ع.ف، وكذلك بمقتضى الفقرة 04 من المادة L.4211-1 من ق.ص.ع.ف.

الفرع الثاني: خضوع بيع المواد الصيدلانية عبر شبكة الانترنيت للاحتكار الصيدلاني

أخضع المشرع الفرنسي بيع الأدوية عبر الإنترنيت لقاعدة الاحتكار الصيدلاني بمقتضى الفقرة 04 من المادة L.4211-1 المعدلة بمقتضى القانون رقم 2014-344 الصادر في 17 مارس 2014[2]، والتي قضت بأن يختص الصيادلة وحدهم بالبيع بالجملة والبيع بالتجزئة التي تتم عن طريق شبكة الإنترنيت، كما عرف التجارة الإلكترونية للأدوية في إطار المادة L.5125-33 من ق.ص.ع.ف.[3] بأنها "كل عملية اقتصادية يقوم بها الصيدلي والذي يقدم أو يضمن عن بعد و عن طريق الإنترنيت البيع بالتجزئة والصرف للجمهور أدوية ذات استعمال بشري، حيث يعمل على توفير المعلومات الصحية على موقعه الإلكتروني، كما أن العملية تتم من الموقع الإلكتروني الخاص بالصيدلية، حيث أن إنشاء واستغلال موقع إلكتروني يكون حصريا من قبل الصيادلة سواء بوصفهم صيادلة أصحاب الصيدلية أو من طرف الصيدلي مدير الصيدلية، كما يمكن استغلال موقع إلكتروني وتشغيله من قبل الصيدلي المساعد، كما يجوز للصيدلي المستخلف استعمال الموقع الإلكتروني للصيدلية حالة وفاة مالك الصيدلية الذي قام بإنشائه.

وإذا كان صرف الأدوية يتم بناء على الوصفة الطبية فهل يجب أن تكون الأدوية التي يتم صرفها عبر الموقع الإلكتروني محل وصفة طبية كذلك؟

---

[1] -Hélène GAUMONT PRAT, directive 2011/62/UE « Médicaments falsifiés » : Les avancées dans la lutte contre les faux médicaments, Op.cit, pp.123-124.

[2] -Art. L.4211-1.C.S.P. modifié par Loi n°2014-344 du 17 Mars 2014.Art.37-38.

[3] -Art. L.5125-33 .C.S.P.modifié par Loi n°2014-201 du 24 Février 2014 portant diverses dispositions d'adaptation au droit de l'union européenne dans le domaine de la santé (1) Art.4.

قضت المادة L.5125-34 المعدلة بمقتضى القانون رقم 2014-201 المؤرخ في 24 فيفري 2014 من ق.ص.ع.ف. [1] بأن لا تكون الأدوية محل العملية التجارية الإلكترونية خاضعة للوصفة الطبية الإلزامية، وعليه فإن الأدوية التي يمكن صرفها عبر الموقع الإلكتروني هي الأدوية التي لا يحتاج صرفها إلى وصفة طبية، أي الأدوية الخاصة ببعض الأمراض والحالات التي يمكن أن لا تكون محل تشخيص طبي ومتابعة طبية.

ورغبة من المشرع الفرنسي في ضبط المواقع الإلكترونية الخاصة بالصيدليات فقد قيد إنشاء الموقع الإلكتروني للتجارة الإلكترونية للأدوية على مستوى الصيدليات بضرورة الحصول على ترخيص من قبل المدير العام للوكالة الجهوية للصحة المختصة إقليميا، كما يلتزم الصيدلي بإعلام المجلس المختص للصيادلة الذي ينتمي إليه بإنشائه للموقع الإلكتروني، وهذا استنادا للمادة L.5125-36 والتي أنشئت بمقتضى الأمر رقم 2012-1427 الصادر في: 19 ديسمبر 2012.[2]

كما يجب أن يتضمن الموقع تفاصيل ومعطيات عن الوكالة الوطنية لسلامة الأدوية ومواد الصحة "ANSMPS" وكذلك رابط تشعبي مع الموقع الإلكتروني للنظام الوطني للصيادلة، والوزارة المكلفة بالصحة وهذا استنادا للمادة R.5125-70 من ق.ص.ع.ف[3] ورغبة كذلك من المشرع في حماية المستهلك المريض من الدواء المزور ومن التجارة غير المشروعة للأدوية عبر مواقع الإنترنيت، فإنه قد وضع في خدمة الجمهور قائمة المواقع الإلكترونية للصيدليات المرخص لها بالتجارة الإلكترونية للأدوية والتي يمكن الاطلاع عليها من خلال الموقع الإلكتروني الخاص بالنظام الوطني للصيادلة وهذا طبقا للمادة R.5125-74 من ق.ص.ع.ف.[4]

وبقصد القضاء على البيع غير المشروع للأدوية عبر الإنترنيت، فقد تمّ طرح مجموعة من العمليات الدولية، منها عملية PANGEAVII" حيث تهدف إلى مكافحة البيع غير المشروع للأدوية عبر الإنترنيت، حيث شاركت فيها سنة 2014، 11 دولة منها: فرنسا، أسفرت هذه

[1]-Art . L.5125-34 C.S.P. modifié par Loi n°2014-201 du 24 Février 2014-Art.4.

[2] -Art. L.5125-36 C.S.P. crée par ord. n°2012-1427 du 19 Décembre 2012.Art.7.

[3] -Art . R.5125-70 C.S.P. crée par décret n°2012-1562 du 31 Décembre 2012-Art.3.

[4] -Art. R.5125-74 C.S.P. crée par décret n°2012-1562 du 31 Décembre 2012-Art.3.

العملية على مصادرة 9.4 مليون دواء مزور، بما يعادل 36 مليون دولار، وغلق 10600 موقع إلكتروني.[1]

المبحث الثاني: المسؤولية الجنائية لبائع المواد الصيدلانية عبر شبكة الإنترنت

تعتبر المسؤولية الجنائية أثر ونتيجة قانونية على الجريمة، ولذلك فكمبدأ عام لإقرار المسؤولية الجزائية في حق البائع عبر شبكة الإنترنت للمواد الصيدلانية يجب أن يصدر عن هذا الأخير ما يعتبر جريمة.

وفي حقيقة الأمر فإن البيع للمواد الصيدلانية على شبكة الإنترنت بحد ذاته يعتبر جريمة في التشريع الجزائري، باعتبار أن المشرع قد استثناها بصريح العبارة بموجب المادة 03 من القانون رقم 18-05 المتعلق بالتجارة الإلكترونية[2].

ولذلك فسنحاول تحديد المسؤولية الجنائية لبائع المواد الصيدلانية من خلال البحث في أساس المساءلة الجنائية لبائع المواد الصيدلانية على شبكة الإنترنت كمطلب أول، في حين سوف نخصص المطلب الثاني لتكييف جريمة بيع المواد الصيدلانية عبر شبكة الإنترنت.

المطلب الأول: أساس المساءلة الجنائية لبائع المواد الصيدلانية على شبكة الإنترنت

يعتبر الخطأ الجنائي ركنا جوهريا لتحقيق المساءلة الجنائية لبائع المواد الصيدلانية عبر شبكة الإنترنت، وهذا ما سنبينه في هذا المطلب، حيث سنحدد الخطأ الجنائي كفرع أول، في حين سنخصص الفرع الثاني لتحديد طبيعته.

الفرع الأول: الخطأ الجنائي

لقد ترك تحديد تعريف الخطأ الجنائي لاجتهاد الفقه ، حيث أغفلت بعض التشريعات تحديده منها قانون العقوبات الفرنسي الصادر عام 1810م، والقانون الألماني الصادر سنة 1870[3]، كما لم يضع المشرع الجزائري هو كذلك تعريفا للخطأ الجنائي.

---

[1] -Hélène GAUMONT PRAT, directive 2011/62/UE « Médicaments falsifiés » : Les avancées dans la lutte contre les faux médicaments, Op.cit. p.127.

[2] القانون رقم 18-05 المؤرخ في 10 ماي 2018، والمتعلق بالتجارة الالكترونية، ج.ر.ع. 28 المؤرخة في16 ماي سنة 2018 .

[3] - طالب نور الشرع ، مسؤولية الصيدلاني الجنائية، دار وائل للنشر و التوزيع، الأردن، ط.01، سنة 2008، ص.53.

ومن التعريفات الفقهية، تعريف الدكتور "حسين فريجة" بأنّه: «كلّ فعل أو امتناع إرادي تترتب نتائج لم يقصدها الفاعل»[1].

كما عرّفه الأستاذ "أحسن بوسقيعة" بأنّه: «تقصير في مسلك الإنسان لا يقع من شخص وجد في نفس الظروف الخارجية».[2]

الفرع الثاني: طبيعة الخطأ الجنائي

ولتقدير الخطأ فقد برز معيارين فقهيان لتقدير الخطأ، وهما المعيار الشخصي والمعيار الموضوعي، ولكن في إطار بيع المواد الصيدلانية على شبكة الإنترنت، فهنا هذا الخطأ إذ قام به بائع صيدلاني هو خطأ مهني، والذي يراد به انحراف الصيدلاني البائع عن الأصول التي تحكم المهنة، وعدم تقيّده بها عند ممارستها، فهو إخلال بواجب من نوع خاص على فئة محددة ينتمون إلى مهنة الصيدلة. [3]

المطلب الثاني: تكييف جريمة بيع المواد الصيدلانية عبر شبكة الإنترنت

سعى التنظيم القانوني الخاص بالمهن الطبية والمواد الصيدلانية، على ضبط التعامل في هذه المنتجات بنصوص آمرة خاصة، كما خص المهن المرتبطة بهذه المنتجات والعمليات الواقعة عليها بشروط قانونية، كما أطّر المشرع التجارة الإلكترونية بقانون خاص، ولهذا فما هو الأساس القانوني لتجريم بيع المواد الصيدلانية عبر شبكة الإنترنت، وما هي أركانها وفيما تمثل العقوبة المقررة لها؟

الفرع الأول: الأساس القانوني لتجريم بيع المواد الصيدلانية عبر شبكة الإنترنت

لقد نص المشرع الجزائري على تجريم بيع المواد الصيدلانية عبر شبكة الإنترنت، في إطار نصوص خاصة منها قانون التجارة الإلكترونية رقم 18-15 بموجب المادة 37 منه، والتي قضى فيها بما يلي: "دون المساس بتطبيق العقوبات الأشد المنصوص عليها في التشريع المعمول به، يعاقب بغرامة من 200.000 دج إلى 1.000.000 دج كل من يعرض للبيع، أو يبيع عن طريق الاتصال الالكتروني المنتجات أو الخدمات المذكورة في المادة 03 من هذا القانون.

---

[1]- حسين فريجة، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية، الجزائر، سنة2006، ص.106.

[2]- أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دار هومة للطباعة والنشر، الجزائر، ط.04، سنة 2006، ص.128.

[3]- منير رياض حنا، المسؤولية الجنائية للأطباء والصيادلة، دار المطبوعات الجامعية، الإسكندرية، ص.44.

يمكن للقاضي أن يأمر بغلق الموقع الإلكتروني لمدة تتراوح من شهر (1) إلى سنة (6) أشهر".

كما نص المشرع في المادة 187 من قانون الصحة رقم 18-11 بأنّه: "تعتبر شبيهة بممارسة غير شرعية للمهنة كل عملية بيع الأدوية أو تخزينها أو إيداعها أو عرضها أو توفيرها على الطريق العمومي، أو في أماكن أخرى غير مرّخص بها... يقوم بها أي شخص ولو كان حائزا شهادة صيدلي"، كما أحال المشرع إلى المادة 243 من ق.ع حيث اعتبر البيع عبر شبكة الانترنيت للمواد الصيدلانية من قبيل الممارسة غير المشروعة لمهن الصحة استنادا للمادة 416 من ق.ص.

الفرع الثاني: أركان جريمة بيع المواد الصيدلانية عبر شبكة الإنترنت والعقوبة المقررة لها

تقوم جريمة بيع المواد الصيدلانية عبر شبكة الإنترنت على ركنين، كما خصّها المشرع بعقوبات، وهذا ما سنحدده من خلال ما يلي:

أولا: أركان جريمة بيع المواد الصيدلانية عبر شبكة الإنترنت

تقوم جريمة بيع المواد الصيدلانية عبر شبكة الإنترنت على ركنين هما:

1- الركن المادي:

يتطلب الركن المادي لجريمة بيع مواد صيدلانية عبر شبكة الإنترنت، توافر شروط وهي:

* **السلوك الإجرامي:** وهنا يتمثل السلوك الإجرامي في قيام أي شخص كان، سواء صيدلي، أو مساعد صيدلي، أو طالب في الصيدلية، أو حتى طبيب، أو شخص غير محترف أصلا في المهن الطبية بفتح موقع الكتروني خاص، سواء كما مرخص به أو غير مرخص بالعرض للبيع، وبيع مواد صيدلانية.[1]
* **النتيجة الإجرامية:** تمثل النتيجة الإجرامية في العمل الذي يقوم به القائم على عملية البيع عبر شبكة الإنترنت، وهو تصريف المواد الصيدلانية عموما والأدوية خصوصا إلى المريض، او تحضير مستحضر صيدلاني بناء على وصفة طبية وصرفه للمريض.

---

[1]- الأمر رقم 66-156، المؤرخ في 8 جوان 1966، يتضمن قانون العقوبات، ج.ر.ع49، الصادرة في 11 جوان 1966، المعدل و المتمم.

* **العلاقة السببية:** وهي التي تربط السلوك الإجرامي بالنتيجة الإجرامية، وذلك باعتبار أن القائم بعملية البيع للمواد الصيدلانية قام بتصريفها وبيعها عبر شبكة الإنترنت.[1]

2- الركن المعنوي:

يتمثل الركن المعنوي في جريمة بيع المواد الصيدلانية في العلم والإرادة، وهنا قد حدد المشرع الفرنسي المواد الصيدلانية التي يجوز بيعها عبر شبكة الإنترنت، وهي المواد التي لا يشترط صرفها بناء على وصفة طبية عبر شبكة الإنترنت في القصد الجنائي، والذي يشمل عنصرين.

والقصد الجنائي يشمل عنصرين وهما العلم والإرادة، ويراد بالعلم هو معرفة التجريم الذي يقع على الفعل، كما يراد بالإرادة هو اتجاه إرادة الصيدلي إلى القيام بعملية بيع المواد الصيدلانية عبر شبكة الإنترنت، وهو يعلم بأنه محضور عليه عملية البيع عبر شبكة الإنترنت.

وعليه ففي جريمة بيع مواد صيدلانية عبر شبكة الإنترنت لا يشترط توافر سوء النية أو قصدا خاصا، حيث تقوم هذه الجريمة بتوفّر القصد العام مع اتجاه إرادته إلى القيام بهذا الفعل على وجه الاعتياد والاستمرار مع علمه بعدم جواز البيع عبر شبكة الإنترنت.

ثانيا: العقوبة المقررة لبائع المواد الصيدلانية عبر شبكة الإنترنت

تعتبر جريمة بيع مواد صيدلانية عبر شبكة الإنترنت شبيهة بالممارسة غير الشرعية للمهنة، استنادا للمادة 187 من ق.ص، واستنادا للمادة 416 من ق.ص، والتي أحالتنا بشأن العقوبة للمادة 243 من ق.ع، فإنه يعاقب كل من يبيع عبر شبكة الإنترنت مواد صيدلانية بـ ثلاثة أشهر إلى سنتين، وبغرامة قدرها 20.000دج إلى 100.000 دج، أو بإحدى هاتين العقوبتين.

[1]- عبد الصبور عبد القوي علي المصري، الجرائم لواقعة ن الصيادلة في القانون المصري و النظام السعودي، جامعة نايف العربية للعلوم الأمنية، الرياض، ط.01، سنة 2013، ص.236.

كما يعاقب كل من قام ببيع أدوية مقلّدة[1] عبر شبكة الأنترنت بالحبس من سنتين (2) إلى خمس سنوات، وبغرامة من 1000.000 دج إلى 5000.000 دج استنادا للمادة 426 من ق.ص.

كما حدد المشرع العقوبة المقررة لبائع المواد الصيدلانية عبر شبكة الانترنت بمقتضى نص خاص في قانون التجارية الإلكترونية رقم 18-05 بمقتضى المادة 37 منه، والتي اشتملت على العقوبة المالية دون السالبة للحرية و التي يسند في تقريرها لقانون العقوبات، والمحددة بغرامة من 200.000 دج إلى 1.000.000 دج، كما يمكن للقاضي أن يأمر بغلق الموقع الإلكتروني لمدة تتراوح من شهر إلى ستة أشهر.

خاتمة:

بالرغم من أن القانون رقم 18-05 المتعلق بالتجارة الإلكترونية و القانون رقم 18-11 المتعلق بالصحة يعتبران حديثا النشأة، غير أن المشرع لم يساير ما توصلت إليه التشريعات الأجنبية بخصوص تأطير عملية بيع الأدوية عبر شبكة الإنترنيت، بل منع أن تكون محل تجارة الإلكترونية ، و رتب المسؤولية الجنائية حالة القيام بذلك.

فالتّطور الذي عرفه العالم ويعرفه، وتطور وسائل الإشهار وظهور الإنترنت، وكثرة القنوات الفضائية التّرويجية، يقتضي غير ذلك، فقد أصبح البيع عبر شبكة الإنترنت يشكّل حصّة الأسد، لذلك يتعيّن على المشرّع الجزائري أن يواكب التّطورات بوضع نصوص قانونية تؤطّر وتنظّم هذا البيع، مثلما فعل المشرّع الفرنسي الذي سبقه القضاء في إخضاع بيع الأدوية على شبكة الإنترنت للاحتكار الصيدلاني وذلك بالنّظر إلى الطبيعة الخطرة لهذه المواد ومكانتها الحيوية.

---

[1]- لقد عرف المشرع الجزائري الأدوية المقلدة بمقتضى المادة 211 من قانون الصحة رقم 18-11، المشار إليه سابقا بأنه":" يقصد بدواء مقلد، في مفهوم هذا القانون، كل دواء معرف في المادة 208 أعلاه، يتضمن خطأ في التقديم بالنسبة:

- لهويته، بما في ذلك ، رزمه ووسمه، و اسمه أو تكوينه....
- لمصدره، بما في ذلك صانعه، بلد صنعه أو بلد منشئه،
- لتاريخه، بما في ذلك التراخيص و التسجيلات و الوثائق المتعلقة بمسارات التوزيع المستعملة."

كما يجب على المشرع أن يقرر نصوصا عقابية تنظم مسألة خرق النصوص المنظمة للتجارة الإلكترونية في مجال المواد الصيدلانية، لا نصوص تحدد العقوبة المقررة لبيع المواد الصيدلانية عبر شبكة الإنترنيت.

الحماية القانونية للمستهلك في ظل المعاملات الإلكترونية

Legal protection for the consumer in light of electronic transactions

د.يوسفي سميرة
جامعة أبوبكر بلقايد- تلمسان- الجزئر.

مقدمة:

أصبحت التجارة الإلكترونية اليوم حقيقة مفروضة على أرض الواقع باعتبارها أحد نتائج العولمة الاقتصادية، فهي حقيقة يعيشها المستهلك والتاجر لما توفره من تسهيلات ومزايا وسرعة معاملات في المجال الاقتصادي والتجاري، أين تلعب شبكة الانترنت دورا فعال في تمكين الشركات من المحافظة على قنوات الاتصال مع الموردين والمستهلكين وكذا القيام بعملية التسويق لمنتجاتها، مع إمكانية توفير رؤية أكثر وضوحا لبرامجها التسويقية.[1]

وكان لظهور الانترنت تأثيرا فعالا في تعديل القواعد القانونية التي تحكم المعاملات القانونية المختلفة بين الأفراد، ومع ظهور الثورة الإلكترونية وتأثيرها على المشرعين في القانون الداخلي والدولي، ظهر ما يسمى بالمعاملات الالكترونية في القانون الخاص كنقيض للمعاملات الكلاسيكية والتي قوامها شبكة الانترنت.[2] وتدخل المشرع الجزائري لأول مرة بتقنين الانترنت كنشاط اقتصادي بموجب المرسوم التنفيذي رقم 257/98[3] المعدل بموجب المرسوم التنفيذي رقم 307/2000[4] الذي يضبط شروط و كيفيات إقامة خدمات الانترنت واستغلالها.

---

[1]- جابر محمد طاهر مشافيه، الحماية المدنية للمستهلك من عيوب المنتجات الصناعية، دار وائل للنشر،2012، ص. 112.

[2]- ناجي فاطمة الزهراء، التجربة التشريعية في تنظيم المعاملات الالكترونية المدنية والتجارية، مداخلة مقدمة المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون المنعقدة في الفترة من 28 إلى 29 أكتوبر 2009، أكاديمية الدراسات العليا، طرابلس.

[3]- المرسوم التنفيذي رقم 257/98 ، المؤرخ في 1998/08/25،الجريدة الرسمية للجمهورية الجزائرية عدد. 63المحدد لشروط و كيفيات إقامة خدمات الإنترنيت،.

[4]- المرسوم التنفيذي رقم 2000/ 307، المؤرخ في 2000/10/14،الجريدة الرسمية للجمهورية الجزائريةعدد. 60، المتعلق بإقامة خدمات الإنترنيت.

هذا ولأول مرة نص المشرع الجزائري على مشروع متعلق بالتجارة الالكترونية من خلال القانون رقم 18-05 المتعلق بالتجارة الالكترونية واعتبرها بموجب الفقرة السادسة من المادة السادسة(6) منه على أنها: " النشاط الذي يقوم بموجبه مورد الكتروني باقتراح أو ضمان توفير سلعة وخدمات عن بعد لمستهلك الكتروني عن طريق الاتصالات الالكترونية."[1]

هذا وتعتبر التجارة الإلكترونية منهج حديث في تنفيذ كل ما يتصل بعمليات بيع وشراء للمنتجات والسلع والخدمات عن طريق تبادل المعلومات باستخدام وسائل الاتصالات دون اشتراط تواجد عملي لأطرافها (المورد والمستهلك)، الأمر الذي خلق بيئة جديدة، قرية عالمية، في عملية التسويق التجاري متمثلة في سوق افتراضية تعتمد على الثقة تتم فيها عملية عرض للمنتجات والخدمات مع تحديد شروط البيع وإجراء مختلف التحويلات المالية فيها.

وبالرغم من المزايا والمنافع الهائلة الناجمة عن عمليات العولمة والتقدم التكنولوجي إلا أنه في ذات الوقت تنجم عنها بعض الانعكاسات والتأثيرات السلبية وظهور أشكال مستحدثة من الجرائم المتعلقة بالغش والاحتيال التي ترتبط بالتسويق الإلكتروني-الرقمي-التي تمثل شكلا جديدا ومميزا للجريمة، حيث أضحت هذه الجرائم تنتشر على نطاق واسع، خاصة بفضل التطور التكنولوجي الذي تستخدمه العصابات الإجرامية لأغراض الغش التجاري ضد المستهلك الإلكتروني لكون هذا الأخير يفتقد معاينة الخدمة والمنتوج محل التعاقد ويعتبر الطرف الضعيف في العلاقة التعاقدية الإلكترونية بالنظر للمهني العالم بخبايا المنتوج وكذا السوق الافتراضية.

هنا تظهر أهمية توفير حماية المستهلك كونه يمثل الطرف الضعيف في العملية التعاقدية في التسويق عامة والتسويق عن طريق الاتصالات بصفة خاصة، فالرغبة في الربح السريع دفعت العديد من التجار والمنتجين ومقدمي الخدمات لإتباع أساليب غير مشروعة لإثراء السريع باستخدام وسائل الغش والخداع المختلفة وهو ما يصطلح عليه بالغش التجاري.

فلا خلاف إذن حول تكريس حماية تشريعية[2] وقضائية فعالة وفعلية لحماية المستهلك الإلكتروني من كل أنواع الغش والتحايل والتظليل في عملية التسويق التي تتم عن بعد. كما لم يكن المشرع

---

[1]- القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439، الموافق ل 10 مايو سنة 2018،الجريدة الرسمية عدد 28، المؤرخة في 30 شعبان عام 1439 الموافق ل 6 مايو سنة 2018 المتعلق بالتجارة الالكترونية.

[2]- الحماية التشريعية تتمثل في الحماية الإدارية والمدنية والجنائية.

الجزائري منعزلا عن الاهتمام العالمي بقضية حماية المستهلك أين تكفل بهذا الموضوع من خلال وضع عدة تشريعات أهمها قانون 09-03 المتعلق بحماية المستهلك وقمع الغش المعدل ولمتمم بالقانون 18-09.[1]

وبناء على ما تقدم سنحاول من خلال هذا البحث تحديد المبادى التي تكرس على أساسها الحماية القانونية فعالة والفعلية للمستهلك الإلكتروني في ظل المعاملات الالكترونية، ومن ذلك نطرح الإشكالية التالية:

في وقت أضحت فيه شبكة الأنترنت تلعب دورا فعالا في عملية التسويق التجاري عبر العالم،أين أصبحت عقود الإستهلاك والمعاملات تبرم عن بعد بواسطة شبكة الاتصالات مما خلق فرص جديدة للمجرمين وسهلت نمو الجريمة الإلكترونية بصفة عامة،ما هو واقع الحماية القانونية للمستهلك الالكتروني في ظل التشريع الجزائري؟ وما هي الحقوق التي تدخل ضمن مصلحة المستهلك الالكتروني؟

وللإجابة عن الإشكالية قيد البحث سوف نتطرق للمفاهيم الأساسية الذي يرتكز عليها السوق الإلكتروني (محور الأول)، بالإضافة إلى حق المستهلك الإلكتروني في الحماية القانونية (محور الثاني).

المحور الأول: مدخل مفاهيمي

تشهد التقنية و التكنولوجيا تطورات كثيرة واستحداث لأمور جديدةخاصة في مجال المعلوماتية التي شهدها العالم مؤخرا، أين تحولت عملية إبرام عقود الإستهلاك من صورتها التقليدية الكلاسيكية القائمة على ضرورة اجتماع كل من المستهلك والمتدخل في مجلس عقد حقيقي إلى تعاقد عملي يتم عن بعد دون ضرورة لحضور الأطراف المعنية،إذ تلعب شبكة الانترنت دورا فعال في العمليات الإلكترونية المبرمة بين المتعاقدين الإلكترونيين،التي تعتبر من أحدث الطرق المستخدمة لاتمام الصفقات وعمليات البيع والشراء في العالم، الأمر الذي خلق بيئة تعامل جديدة في عملية التسويق التجاري.

---

[1]- القانون رقم 18-09 المؤرخ في 25 رمضان عام 1439 الموافق ل 10 يونيو سنة 2018، يعدل ويتمم القانون رقم 09-03المؤرخ في 25فبراير 2009،الجريدة الرسمية عدد 35، المؤرخة في 28 رمضان عام 1439 لموافق ل 13 يونيو سنة 2018المتعلق بحماية المستهلك وقمع الغش.

هذا و كان لظهور الأنترنت والتطور التكنولوجي والتقني تأثير فعال في تعديل القواعد القانونية التي تحكم المعاملات المختلفة بين الأفراد وكذا في ظهور مصطلحات جديدة تتعلق بالسوق الإلكترونية والمتعاملين فيها، الأمر الذي دفع المشرع الجزائري بوضع قانون خاص ينظم ويضمن أمن التجارة الالكترونية، وهو القانون رقم 18-05 المتعلق بالتجارة الالكترونية.

سنحاول في هذا المحور التطرق للمفاهيم والمصطلحاتالأساسية المتعلقة بالبيئة والتسويق الإلكترونيين.

أولا: السوق الإلكترونية:

تعتبر السوق الالكترونية البيئة الافتراضية للتسويق الالكتروني المكان الذي يتم فيه الاتصال المباشر للأجهزة الذكية مع شبكة الأنترنيت بغرض التسويق، ويعني فضاء الأنترنيت ترابط حواسيب وأجهزة ذكية مع أنظمة اتوماتيكية.

ويعرف الواقع الافتراضي أو الواقع التقريبي، محاكاة يولدها الحاسوب لمناظر ثلاثية الأبعاد بمحيط أو سلسلة من الأحداث تمكن الناظر الذي يستخدم جهازا الكترونيا خاصا من أن يراها على شاشة عرض ويتفاعل معها بطريقة تبدو فعلية.[1]

هذا وقد تطرق المشرع الجزائري في أول مشروع يتعلق بالتجارة الالكترونية لتعريفها على أنها "النشاط الذي يقوم بموجبه مورد الكتروني باقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك الكتروني عن طريق الاتصالات الالكترونية."[2]

تعني البيئة الإلكترونية التجارية ما يعرف بالسوق الإلكترونية أو الواقع الافتراضي للسوق الحقيقية والمكان الذي تتم فيه العمليات التجارية بطريقة معلوماتية ما أدى إلى ظهور قرية عالمية، وهنا يتم خلق بيئة اقتصادية بطريقة ذكية تكون فيها عملية العرض والطلب للسلع و المنتوجات والخدمات[3]بطريقة الكترونية تتم بإدخال وعرض المعلومات والصور للمنتجات والسلع والخدمات في فضاء الذي يكون له اتصال مباشر بشبكة الانترنت باستعمال الأجهزة الذكية ما

1- معجم المعاني الجامع، معجم عربي عربي. قاموس المعجم الوسيط، اللغة العربية المعاصرة، الرائد، لسان العرب، القاموس المحيط، قاموس عربي عربي.

2- المادة 6 الفقرة الأولى من القانون 18-05 المتعلق بالتجارة الالكترونية.

3- الخدمة الالكترونية مهمة يمون فيها التسهيل على الافراد سواء طبيعية أو معنوية مسألة التنقل والوقت وغيرها من الخدمات العادية لكن عن بعد غير الخدمات التقليدية.

يجعل المنتج أو السلعة أو الخدمة محل التعاقد تظهر على صورتها الحقيقية، يصطلح عليه بالتسويق الالكتروني ما يخلق عالم افتراضي حقيقي في مجال التسويق التجاري تتم فيه المعاملات والعقود الالكترونية بيع وشراء بعيدا عن الحضور الحقيقي لأطراف العقد في مجلس التعاقد.

هذا ويعرف العقد الالكتروني بمفهوم القانون رقم 04-02 المؤرخ في جمادى الأولى عام 1425 الموافق 23 يونيو سنه 2004 الذي يحدد القواعد المطبقة على الممارسات التجارية، وهو عقد يتم إبرامه عن بعد، دون الحضور الفعلي والمتزامن لأطرافه باللجوء حصريا لتقنية الاتصال الالكتروني.[1]

ورغم أن بعض المستهلكين قد يرفضون التعامل بالتكنولوجيات لمخاوفهم من التعرض للغش والاحتيال، فإن اتساع حجم التجارة الالكترونية أصبح ليس بالإمكان إيقافه نظرا للمزايا والسرعة التي تتم بها هذه المعاملات الإلكترونية بدون تكبد عناء التنقل لمجلس العقد. وكذا لما يحققه هذا النشاط التجاري الإلكتروني من أرباح كبيرة مقارنة بما كان يحققه بشكله التقليدي، لذا يجب أن تتوفر في كل المتعاملين الالكترونيين بما فيهم المستهلك الثقة في التعامل والحفاظ عليها خاصة أن المعاملات الالكترونية تتم بعيدا عن مجلس العقد.

ثانيا: المستهلك الإلكتروني:

لم يعرف المشرع الجزائري المستهلك الالكتروني إلا بعد صدور القانون 18-05 المتعلق بالتجارة الإلكترونية أين إعتبره كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الاتصالات الالكترونية من المورد الالكتروني بغرض الاستخدام النهائي.[2]

والمستهلك الإلكتروني نفسه المستهلك العادي،[3] إذا ما قراناهما معا، لكن عملية إشباع غريزته الاستهلاكية تختلف عن الطريقة الكلاسيكية أين يتم التعاقد بشأن السلع والخدمات المعروضة

---

[1]- المادة 6 الفقرة الثانية من القانون 18-05 المتعلق بالتجارة الالكترونية.

[2]- المادة 6 الفقرة الثالثة من القانون 18-05 المتعلق بالتجارة الالكترونية.

[3]- عرف المشرع الجزائري المستهلك في المادة 3 من القانون 09-03 المتعلق بحماية المستهلك وقمع الغش المعدل والمتمم بالقانون 18-09، على أنه: " كل شخص طبيعي أو معنوي يحصل بمقابل أو مجانا على سلعة أو خدمة موجهة للاستعمال النهائي من أجل إشباع حاجاته الشخصية أو تلبية حاجة شخص آخر أو حيوان متكفل به."

للتسويق بطريقة عملية بعيدا عن مجلس العقد، باستخدام وسائل الاتصال الإلكترونية التي تربط شبكة الانترنيت والأجهزة الذكية معا.[1]

بناء على ما تقدم فالمستهلك الالكتروني هو كل شخص طبيعي أو معنوي مقتن لسلعة أو خدمة بصفة نهائية[2]باستخدام الاتصالات الالكترونية غير الطريقة العادية.

تتعلق مصلحة المستهلك بالدرجة الأولى بحصوله على المنتجات والخدمات التي تلبي احتياجاته وإشباع رغباته مقابل ثمن يقدمه المستهلك الإلكتروني يدخل ضمن التزامهأمام المورد الكتروني[3] وعلى الدولة أن تكفل له هذا الحق، فعنى حماية المستهلك العادي أو الإلكتروني تضمن حقوقه التي لابد من ترسيخها وضبطها في الاقتصاد الوطني.

هذا ويلتزم المستهلك الالكتروني بتوقيع وصل الاستلام عند التسليم الفعلي للسلعة أو عند التأدية الفعلية للخدمة موضوع العقد الالكتروني، بحيث لا يمكن للمستهلك الإلكتروني رفض التوقيع عند تسلمه محل العقد الالكتروني من قبل المورد أو من ينوب عنه في توصيل محل التعاقد.[4]

ثالثا: المورد الالكتروني:

عرف المشرع الجزائري المورد الإلكتروني في القانون 18-05 المتعلق بالتجارة الالكترونية على أنه:"كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير السلع أو الخدمات عن طريق الاتصالات الالكترونية".[5]وبمقارنة المورد الإلكتروني مع المورد العادي[6] نجد أن طريقة تدخل

---

[1]- الأجهزة الذكية مثل الحاسوب، الهواتف النقالة الذكية، اللوحات الذكية...

[2]- الاستهلاك بصفة نهائية بمعنى أنه لا يهدف إلى إعادة بيعها أو تحويلها أو استخدامها في نشاطه المهني.

[3]- المادة 16 من القانون 18-05 المتعلق بالتجارة الالكترونية تنص على أنه: "ما لم ينص العقد الإلكتروني على خلاف ذلك، يلتزم المستهلك الالكتروني بدفع الثمن المتفق عليه في العقد الالكتروني بمجرد إبرامه".

[4]- المادة 17 من القانون 18-05 المتعلق بالتجارة الالكترونية تنص على: "يجب على المورد الالكتروني أن يطلب من المستهلك الالكتروني توقيع وصل استلام عند التسليم الفعلي للمنتوج أو تأدية الخدمة موضوع العقد الالكتروني؛ لا يمكن للمستهلك الالكتروني أن يرفض توقيع وصل الاستلام؛ تسلم نسخة من وصل الاستلام وجوبا للمستهلك الالكتروني".

[5]- المادة 6 الفقرة الرابعة من القانون 18-05 المتعلق بالتجارة الالكترونية.

[6]- عرف المشرع الجزائري المورد العادي في كل من:

المادة 3 الفقرة 8 من القانون رقم 03/09 المتعلق بحماية المستهلك وقمع الغش المعدل والمتمم بالقانون 18-09 على أنه "كل شخص طبيعي أو معنوي يتدخل في عملية عرض المنتوجات للاستهلاك".

المورد الإلكتروني في عملية التسويق أي عرض المنتجات والسلع والخدمات تتم باستخدام الاتصالات الالكترونية عكس الطريقة العادية التي يتدخل بها المورد العادي.

الأمر الذي يُمكن المتدخل نتيجة خبرته بالعلم والدراية الكافية بخبايا الخدمة و المنتوج وكذا السلعة التي يعرضها على المستهلك الإلكتروني، في المقابل يفتقد المستهلك الالكتروني لمعاينة الخدمة أو السلعة أو المنتوج محل التعاقد كونه يعتمد على ما يقدمه المهني من معلومات وصور إلكترونية فقط.

هنا يًظهر المهني الإلكتروني أساس الثقة في السوق الإلكترونية الافتراضية مما يلزمه تقديم المعلومات الصحيحة والدقيقة المتعلقة بالتسويق.وبمجرد إبرام العقد الالكتروني يعد المورد الالكتروني مسؤولا بقوة القانون أمام المستهلك الالكتروني عن حسن تنفيذ الالتزامات المترتبة على هذا العقد من دون المساس بحقه في الرجوع ضدهم. كما يًمكن للمورد الإلكتروني أن يتحلل من كامل المسؤولية أو جزء منها إذا أثبت أن عدم تنفيذ العقد الالكتروني يعود إلى المستهلك الالكتروني أو إلى قوة قاهرة.[1]

هذا ويجب على المورد الالكتروني بمجرد ابرام العقد أن يرسل نسخة إلكترونية منه للمستهلك الإلكتروني.[2] كما يترتب عليه إعداد فاتورة على كل بيع أو تأدية خدمة على أن تسلم للمستهلك الالكتروني.[3]

رابعا: الجريمة الإلكترونية الواقعة على المستهلك:

يطلق عليها الجريمة الإلكترونية أو المعلوماتية أو السبيرانية[4] ويعرف الفضاء السيبراني أو الإلكتروني، بالمجال المجازي لأنظمة الحاسوب والشبكات الإلكترونية حيث تخزن المعلومات

كما عرفه المشرع في المادة 2 من المرسوم التنفيذي رقم 90\266 المؤرخ في سبتمبر 1990 المتعلق بضمان المنتوجات والخدمات، على أنه: " كل منتج أو صانع، أو وسيط أو حرفي، أو تاجر أو مستورد، أو موزع وعلى العموم كل متدخل ضمن إطار مهنته في عملية عرض المنتوج أو الخدمة للاستهلاك ".

[1]- المادة 18 من القانون 18-05 المتعلق بالتجارة الالكترونية.

[2]- المادة 19 من القانون 18-05 المتعلق بالتجارة الالكترونية.

[3]- المادة 20 من القانون 18-05 المتعلق بالتجارة الالكترونية.

[4]- الجرائم السبيرانية من سيبر ويعني فضاء الانترنت كما تعني ترابط الحواسيب مع أنظمة أوتماتيكية.

إلكترونيا، وتتم الاتصالات المباشرة على الشبكة، وإذا ما وردت عبارة الجريمة الحاسوبية أو جريمة الاتصالات والمعلوماتية فهي تعني الجريمة السيبرانية.[1]

والجريمة الالكترونية أو التقنية تميز عن الجريمة التقليدية في كون الجريمة الإلكترونية تستعمل فيها أداة ذات تقنية عالية وكذا مكان الجريمة يكون عن بعد أين لا يشترط انتقال الجاني ماديا بل تتم الجريمة عن بعد بواسطة شبكة النت تربط بين الجاني والمستهلك.[2]تتشابه الجريمتين التقليدية والإلكترنية في كونهما كأي جريمة تحتوي على طرفين أحدهما له صفة الجاني وهو المتدخل الإلكتروني والمجني عليه الذي له صفة المستهلك الإلكتروني.

هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أو الأجهزة الذكية الموصولة بشبكة الانترنيت بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامي.

يقوم الركن المادي للجريمة الإلكترونية المرتكبة ضد المستهلك الإلكتروني بإتيان سلوك إيجابي أو سلبي من شأنه المساس بأمن وسلامة المستهلك الإلكتروني، مع اشتراط أن تكون بيئة التعامل وسط إلكتروني.

أما عندما يتعلق الأمر بالركن المعنوي في الجريمة الإلكترونية، فإن الأساس الذي يقوم عليه الركن المعنوي للجريمة الواقعة على المستهلك هو توافر إرادة آثمة لدى المتدخل أو المهني الإلكتروني مع ضرورة توجه هذه الإرادة إلى إتيان السلوك غير المشروع والمجرم قانونا، كالإيهام بجودة المنتوج أو السلعة بالرغم من رداءتها رغم علم المتدخل بالآثار الضارة المنجرة عن استعمالها بغرض استنزاف أموال المستهلك الإلكتروني، لحد الذي صار معه بعض الفقه يصطلح على إجرامية الاستهلاك الواقعة بالبيئة الالكترونية بالهجوم الإلكتروني الواقع على المستهلك.[3]

---

[1]- نوال مجدوب، الحماية الجنائية والإدارية للمستهلك في عملية التسويق، رسالة دكتوراه في القانون الخاص، تخصص القانون الجنائي للأعمال، جامعة أبو بكر بلقايد تلمسان، 2017، الصفحة 120.

[2]- محمد السالم عباد، شرح قانون العقوبات، ط.01، مكتبة دار الثقافة، الأردن، ص.232،231.

[3]- زايري بلقاسم ودلوباشي علي، طبيعة التجارة الالكترونية وتطبيقاتها المتعددة، المؤتمر العلمي السنوي الثاني لتكنولوجيا المعلومات ودورها في التنمية الاقتصادية، كلية الاقتصاد والعلوم، 2002، ص.361،360.

المحور الثاني: حق المستهلك الالكتروني في الحماية القانونية:

نشأت التكنولوجيات والتقنيات الجديدة وتوفرها على نطاق واسع بالرغم من منافعها الكثيرة إلا أنها اتاحت ارتكاب جرائم بوسائل حديثة ولابد من فهم جديد لهذه الجرائم المستحدثة وابتكار وسائل جديدة ومتقدمة لفهما ومواجهتها ما يتطلب استعدادا فكريا وتأهيلا وتدريبا خاصا.[1]

يبقى المستهلك أساس العلاقة في البيئة الاقتصادية والتجارية سواء الإلكترونية أو التقليدية فمن الضروري توفير الحماية والأمن لسلامة المستهلك هنا تكمل مصلحة المستهلك الذي يعتبر الطرف الضعيف في المعادلة الاقتصادية بالمقارنة مع المتدخل أو المورد. فلا بد من توفير وتأمين الحماية له من الأضرار الناتجة عن العلاقة التجارية التي من شأنها أن تضر بمصلحة المستهلك الاقتصادية سواء المالية[2] أو الصحية والتي ممكن أن تتضرر بتخلف عنصر من عناصر الخدمة خاصة في المعاملات وعقود الاستهلاك الإلكترونية المبرمة عن بعد في واقع افتراضي والتي تتم دون لقاء مباشر بين الأطراف المعنية، أيضا لا تتم فيها معاينة السلعة أو الخدمة بطريقة مباشرة، فالعرض والطلب كلاهما يتم عن طريق الأنترنت أي عن بعد.

فكرة حماية المستهلك الإلكتروني إذن تكمل في حماية مصالحه ويبقى هذا الموضوع دون أهمية مالم تبنى هذه الفكرة على قواعد وأحكام قانونية وإجراءات تستمد منها مرجعيتها، فمسألة حماية المستهلك أمر بالغ الأهمية خصوصا في ظل تعاظم الانتهاكات المرتبطة بحقوقه من جهة وعجز الجهود الفردية من جهة أخرى، والمخاطر التي يتعرض لها المستهلك قد يكون مصدرها التاجر أو المنتج الذي يمثل الطرف الآخر في العلاقة التعاقدية الذي كثيرا ما يتسم سلوكه بالغش والتحايل والخداع ليكتشف المستهلك الالكتروني أنه ضحية السلعة التي يقتنيها أو الخدمة محل تعاقده.

بناء على هذا الطرح سوف نتطرق لحماية المستهلك الإلكتروني في النقاط التالية:

أولا: حق حماية المستهلك من الأفعال المجرمة.(الغش والخداع)

---

[1]- أيمن صقر، مجلة الشرق، الجريمة السيبرانية من التحديات الكبرى التي تواجه المجتمع القانوني، مؤتمر الأمم المتحدة 13 لمنع الجريمة والعدالة الجنائية، الدوحة 17 أبريل 2015، الجلسة العامة للمؤتمر، الساعة 21:30.

نتيجة التطور الكبير والسريع للأجهزة وضعف القدرة على المرافقة والمراقبة والتحكم خاصة في ظل إبرام عقود الإستهلاك الإلكترونية الذي يتم بصورة افتراضية، فإن المستهلك الإلكتروني أصبح عرضة لمخاطر صور إجرامية عديدة، ويعد الغش والخداع الإلكترونيين من أهم صور الإجرامية الواقعة على المستهلك في البيئة الإلكترونية.

فإذا كان من السهل بالأمس إثبات أن المستهلك تعرض للغش أو الخداع أو التظليل في عقود الإستهلاك العادية، فإنه اليوم صار من الصعب إثبات الاعتداء الذي يتعرض له المستهلك الإلكتروني، فإنه لا إشكال أن نثبت تعرض المستهلك للغش في عقود الإستهلاك بمجرد إثبات أن البائع في البيئة التقليدية عرض منتوجا مغشوشا أو فاسدا أو مسموما للتسويق، إلا أن المسألة تأخذ بعدا آخر في ما يخص الغش والخداع الإلكتروني، إذ أن عملية العرض والوضع للبيع أو الخدمة لا يتم بصورة تقليدية بل بصورة افتراضية، مما يصعب معه إثبات العدوان الذي من الممكن أن يعتمده المتدخل من أجل تحقيق ربح بطرق غير مشروعة التي تظهر الخدمة أو السلعة على غير حقيقتها والتي من شأنها أن تمس باستغلال وضعف أو جهل المستهلك الإلكتروني بغرض استنزاف أموال المستهلك الإلكتروني بصورة غير شرعية أين نتضرر مصلحته المالية وأحيانا حتى صحته وسلامته الشخصية.

يعتبر الغش والخداع المرتبطان بالتجارة الالكترونية أحد أشكال الجرائم الالكتروني، وفي نفس الوقت أحد أشكال الجرائم الاقتصادية، ومنه فإن الغش والخداع التجاري عبر الانترنت يقع ضمن الغش التجاري التقليدي وكذا داخل الجريمة الالكترونية، ما يجعلنا في ظل غياب هذيتن الجريمتين في القانون 18-05 المتعلق بالتجارة الالكترونية أن نتعرض للجريمتين طبقا للقواعد العامة.

فالمشرع الجزائري وفر الحماية الجنائية من جريمتي الغش والخداع في عملية التسويق، ما يظهر في النصوص القانونية على النحو الآتي:

الخداع التجاري نجد تجريمه في كل من نص المادة 429 من قانون العقوبات،[1] وكذا نص المادة 68 من القانون 09-03 المتعلق بحماية المستهلك وقمع الغش[2]، وهو تصرف من شأنه إيقاع المتعاقد في الغلط حول البضاعة أو الخدمة، أي أن يقوم المتدخل بأعمال من شأنها إظهار السلعة أو المنتوج أو الخدمة على غير حقيقتها.[3]

وتفترض جريمة الخداع بمجرد عرض سلع ومنتجات وخدمات مخدوعة وغير مطابقة من حيث مصدرها أو تركيبتها أو منشئها... الأمر الذي يتوافق مع مبدأ الاحتياط، باعتبار أن جرائم الاستهلاك من جرائم الخطر لا من جرائم الضرر.

---

[1]- المادة 429 من قانون العقوبات تنص على أنه: "يعاقب كل من يخدع أو يحاول أن يخدع المتعاقد...".

[2]- المادة 68 من القانون رقم 09-03 المتعلق بحماية المستهلك وقمع الغش المعدل والمتمم بالقانون رقم 18-09، تنص على أنه: "يعاقب بالعقوبات المنصوص عليها في المادة 429 من قانون العقوبات كل من يخدع أو يحاول أن يخدع المستهلك بأية وسيلة أو طريقة كانت حول:

- كمية المنتوجات المسلمة،
- قابلية استعمال المنتوج،
- تاريخ أو مدد صلاحية المنتوج،
- النتائج المنتظرة من المنتوج،
- طرق الاستعمال أو الاحتياطات اللازمة لاستعمال المنتوج".

[3]- مجدوب نوال، حماية المستهلك جنائيا من جريمة الخداع في عملية تسويق المواد الغذائية، مجلة دفاتر السياسة والقانون، العدد 15، جوان 2016، ص.270.

الغش التجاري نجد تجريمه في كل من نص المادة 431 من قانون العقوبات،[1] وكذا نص المادة 70 من القانون 09-03 المتعلق بحماية المستهلك وقمع الغش،[2] وهو كل فعل من شأنه أن يغير من طبيعة المواد أو فائدتها بغض النظر عن الوسائل التي لجأ أليها المتدخل في سبيل تحقيق غايته. وتعد جريمة الغش من جرائم الخطر لا جرائم الضرر، أي أن الجريمة متوافرة وقائمة بمجرد حلول الخطر دون الحاجة لانتظار وقوع الضرر.[3] الهدف من حماية المستهلك جنائيا ضد الغش في عملية التسويق هو حماية الصحة العامة بالدرجة الأولى.

يعتبر جاني في جريمة الغش كل متدخل في عملية تسويق لسلعة أو منتوج أو خدمة مغشوشة أو فاسدة أو مسمومة، هذا ضمانا لحماية فعالة وفعلية لمستهلك الذي قد يكون ضحية متضرر من الغش. والغرض من حماية المستهلك من الخداع والغش هو حماية الثقة والنزاهة في المعاملات التجارية بصفة عامة والمعاملات الإلكترونية بصفة خاصة.

ومنه مصالح حماية المستهلك الإلكتروني تمثل في حصوله على السلع والخدمات خالية من الغش والخداع والتحايل، وكذا السلع والخدمات المطابقة للمواصفات من حيث الكم والكيل والوزن والقياس، وأن تكون على درجة عالية من الجودة والأمن، وحقه أيضا في الحصول على معلومات

---

[1]- المادة 431 من قانون العقوبات تنص على أنه: "يعاقب كل من:

- يغش مواد صالحة لتغذية الإنسان أو الحيوانات أو مواد طبية أو مشروبات أو منتوجات فلاحية أو طبيعية مخصصة للاستهلاك،

- يعرض أو يضع للبيع أو يبيع مواد صالحة لتغذية الإنسان أو الحيوانات أو مواد طبية أو منتوجات أو مشروبات أو منتوجات فلاحية أو طبيعية يعلم أنها مغشوشة أو فاسدة أو مسمومة

- يعرض أو يضع للبيع أو يبيع مواد خاصة تستعمل لغش مواد صالحة لتغذية الإنسان أو الحيوانات أو المشروبات أو المنتوجات الفلاحية أو طبيعية أو يحث على استعمالها بواسطة كتيبات أو منشورات أو نشرات أو معلقات أو إعلانات أو تعليما مهما كانت".

[2]- المادة 70 من القانون رقم 09-03 المتعلق بحماية المستهلك وقمع الغش المعدل والمتمم بالقانون رقم 18-09، تنص على أنه: "يعاقب بالعقوبات المنصوص عليها في المادة 431 من قانون العقوبات كل من:

- يزور أي منتوج موجه للاستهلاك أو الاستعمال البشري أو الحيواني،

- يعرض أو يضع للبيع أو يبيع منتوجا يعلم أنه مزور أو فاسد أو سام أو خطير للاستعمال البشري أو الحيواني،

- يعرض أو يضع للبيع أو يبيع، مع علمه بوجهتها مواد أو أدوات أو أجهزة أو كل مادة خاصة من شأنها أن تؤدي إلى تزوير أي منتوج موجه للاستعمال البشري أو الحيواني".

[3]- مجدوب نوال، الحماية الجنائية والإدارية للمستهلك في عملية التسويق، المرجع السابق، ص.19.

صادقة حول السلع والخدمات فيما تقدم ذكره، وأن تكون السلعة متوفرة في الأسواق وبأسعار مناسبة،[1] ويعتبر ما يخالف ذلك خرقا وفعلا مجرما في حق المستهلك العادي والمستهلك الإلكتروني معا.

ثانيا:حق حماية إعلام المستهلك الإلكتروني.

إن الالتزام بالإعلام من أكبر الآليات القانونية التي ينبغي المطالبة بها في مجال حماية المستهلك العادي والالكتروني لضمان حماية أوسع للمستهلك في إطار معالجة مسألة عدم التكافؤ في المركز القانوني بين أطراف العقد (المورد والمستهلك).

أما المشرع الجزائري فقد أشار إلى الالتزام بالإعلام الالكتروني كأول مرة من خلال نصه في المادة 17 من القانون 09-03 المتعلق بحماية المستهلك وقمع الغش، بقوله: "يجب على كل متدخل أن يعلم المستهلك.... بأية وسيلة أخرى مناسبة." يقصد المشرع بذلك اعلام حول المنتوجات بأية وسيلة بما في ذلك الطرق التكنولوجيا الحديثة.[2]

لم يغفل المشرع الجزائري بالنص في القانون 18-05 المتعلق بالتجارة الالكترونية على الإشهار الإلكتروني بتنظيمه لأحكام خاصة وبالتحديد في المادة السادسة الفقرة السادسة منه على أنه: "كل إعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع سلع أو خدمات عن طريق الاتصالات الالكترونية."[3]

الإعلام الإلكتروني هو حق يقع على عاتق المورد الإلكتروني لإعلام وتبصير المستهلك الإلكتروني بالمعلومات الشاملة عن كل ما يتعلق بعملية البيع عبر شبكة الاتصالات أو أية وسيلة

---

[1]- فاطمة بحري، فاطمة بحري، الحماية الجنائية للمستهلك، بحث مقدم لنيل دوحة دكتوراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2012-2013، ص.56.

[2]- المادة 3 الفقرة 15 من المرسوم التنفيذي رقم 14-378 المؤرخ في 5 محرم عام 1435 الموافق ل9 نوفمبر سنة 2013، الجريدة الرسمية رقم 58 المؤرخة 14 محرم عام 1435 الموافق ل 18 نوفمبر سنة 2013، الذي يحدد الشروط والكيفيات المتعلقة بإعلام المستهلك.

[3] - المادة 6 الفقرة 6 من القانون 18-05 المتعلق بالتجارة الالكترونية.

أخرى حتى يكون المستهلك على بينة من أمره بحيث يتخذ قراره الذي يراه مناسب على ضوء حاجته وهدفه من إبرام العقد الإلكتروني.[1]

يهدف الحق في الإعلام بتحقيق حماية الإرادة التعاقدية للمستهلك، كما يحقق حماية فكر المستهلك وثقافته. ويجب على المورد أن يعلم المستهلك قبل إبرام العقد بالمميزات الجوهرية للسلعة أو الخدمة،[2] أين يلتزم المورد أيضا بأن يرفق المنتج بكل المعلومات اللازمة، ويعد الكذب والتظليل في الإعلان التجاري من أهم مصادر الأضرار التي قد تلحق بالمستهلك خلال الفترة التي تسبق إبرام العقد.

على هذا الأساس تستدعي الضرورة حماية المستهلك بإعلامه وهي الضرورة التجارية حتى يتسنى للمستهلك الإلكتروني أن يكون على بينة من أمره خاصة بعد أن أضحى اكتظاظ الأسواق بالعديد من السلع والمنتجات المتنوعة التي تجعل المستهلك في حيرة لاختيار المنتوج الأصلح له.[3]

كذلك هو الإعلان في قوانين حماية المستهلك هو الإعلان الذي يؤدي إلى تزويد المستهلك بمعلومات صحيحة ووافية وواضحة، تتناول البيانات الأساسية للسلعة أو الخدمة وطرق الحصول عليها واستخدامها. وتباعد المتعاقدين وانتشار الإعلانات الخادعة المفترضة في العقود الإلكترونية، وتباين الخبرات الفنية، توسع من دائرة الاختلال الفادح بالتوازن العقدي، مع استغلال طيش المستهلك الإلكتروني في التعاقد الإلكتروني واندفاعه نحو الإعلانات الخادعة والسلع المفترضة، ما يجعل العقد قابل للإبطال لعيب من عيوب الإرادة وهي الغلط، التدليس، الإكراه، الاستغلال.

هذا ونجد أن غالبية عقود نشر الإعلانات التي تتم عبر شبكة الإنترنت تضمن بندا يلزم المعلن أن يحترم قواعد السلوك المرتبطة بالعقد والتي تحظر الكذب والتضليل في الإعلانات التجارية،

---

[1]- عمارة مسعودة، الحماية المدنية للمستهلك في مرحلة ما قبل التعاقد الالكتروني من خلال الإعلان التجاري الكاذب والحق فب الإعلام، مجلة البحوث والدراسات القانونية والسياسية، مجلة كلية الحقوق، جامعة سعد دحلب، البليدة، العدد الثاني، صفر عام 1433 الموافق ل جانفي سنة 2012، ص.327.

[2]- فاطمة بحري، الحماية الجنائية للمستهلك، المرجع السابق، ص.58.

[3]- دليلة معزوز، الالتزام بإعلام المستهلك الالكتروني ومدى فاعلية وشمولية قانون 09-03 المتعلق بحماية المستهلك وقمع الغش، مجلة المعارف، السنة الخامسة، العدد الثامن، جوان 2010، ص.80.

وتضمن حق العدول عن العملية التعاقدية خصوصا في الإعلانات التي يتم الدفع فيها بعد استلام محل العقد الإلكتروني.

ثالثا: حق حماية صحة وسلامة المستهلك:

حماية مصالح المستهلك يهدف بها المشرع لحماية المصلحة الاقتصادية للدولة هنا ظهرت الحاجة إلى حماية الطرف الضعيف في حلقة التعاقد باعتباره أساس العلاقة التعاقدية. ومصلحة المستهلك في حماية سلامته وصحته حق تعمل على تحقيقه الدولة بتدخلها وفرضها لإجراءات قانونية وردعية وسن قوانين جنائية لقمع الجرائم التي تضر أو تهدد صحة وسلامة وأمن المستهلك. وتصدى المشرع الجزائري لفعل الخداع والغش، وضمن حماية في كل من قانون العقوبات[1] وقانون حماية المستهلك من كل عدوان يقع على المستهلك سببه الغش والخداع وكذا القانون رقم 18-05 المتعلق بالتجارة الالكترونية، بل وشدد العقوبات في حالة ما أدى الضرر إلى إحداث عاهات مستديمة أو إلى الوفاة.

من هنا تظهر أهمية ثقة المتدخل ومسؤوليته في ضمان صلاحية محل تعاقد الالكتروني على أن يكون صالح للغرض الذي أعد من أجله وخال من العيوب الخفية التي من الممكن أن تشوبه، لذا وجب على المتدخل أو عارض السلعة أن يضمن عيوبها التي تنقص من قيمتها نقصا محسوسا أو التي تجعلها غير صالحة للاستعمال فيما أعدت لها بحسب طبيعة العقد، فحق سلامة المنتوجات والخدمات تدخل ضمن نظرية الالتزام والعقود. ففي حالة انعدام سلامة المنتوج غير صالح لتحقيق الغرض المخصص له قد تؤثر سلبا على سلامة وصحة المستهلك العادي والإلكتروني معا مما يؤدي إلى الإضرار به، وهنا تقوم مسؤولية المتدخل أو عارض المنتوج أو الخدمة محل التعاقد.

كان للمشرع تدخل واضح بفرض إجراءات قانونية وردعية وسن قوانين جنائية لقمع الجرائم التي تضر أو تهدد المصلحة المستهلك لذا أوجب على المتدخل إعلام المستهلك بكل ما يحيط بالمنتوج أو السلعة أو الخدمة على النحو الذي يسمح له بحرية الاختيار، مما يقع على المتدخل ضمان سلامة

---

[1]- القانون رقم 02/16، المؤرخ في 19 يونيو 2016، المعدل والمتمم للأمر رقم 156/66، المؤرخ في 08 يونيو 1966، والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد.37، الصادرة في 22 يونيو 2016.

المنتوج وعدم إضراره بحياة وصحة المستهلك. وكل ما يقال عن المستهلك التقليدي يطبق على المستهلك الالكتروني في ظل عدم وجود نصوص قانونية خاصة بالمستهلك الالكتروني، وإلى غاية النص على ذلك.

خاتمة:

تشهد التقنية والتكنولوجيا تطورات كثيرة واستحداث لأمور جديدة، هذا الأمر ينذر بتطور أدوات وسبل الجريمة الإلكترونية بشكل أكثر تعقيدا أو أشد ضررا من قبل، الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم واستحداث خطوط دفاع وسن قوانين وتوعية الناس بمستحدثات هذه الجرائم وتشجيعهم للإبلاغ عنها.

من حيث المبدأ تضمنت المنظومة القانونية نصوص صريحة تجرم كل سلوك منافي للقانون في البيئة الإلكترونية، إلا أنها تبقى محدودة من منطلق أن المشرع اكتفى بوضع حجر الأساس للإجرام الإلكتروني أو المعلوماتيالماس بالمستهلك، مع صعوبة إثبات الضرر الذي قد يطال المستهلك الإلكتروني، من منطلق أن المتدخل الإلكتروني أكثر خبرة وحنكة وتمرن بأصول التسويق الإلكتروني، ومن ثم سيطمس كل الأدلة. ولم يواصل المشرع مسيرة التجريم والعقاب رغم تزايد الإجرام في هذا المجال بشتى صوره أين أصبحت هذه الجرائم في وقتنا الراهن تهدد أمن وسلامة الأفراد أو المؤسسات أو حتى الحكومات، هو ما يقتضي الإسراع في اتخاذ الإجراءات اللازمة التي من شأنها التقليل من حدة هذا النوع من الجرائم.

ينبغي أيضا العمل على التصدي للأشكال الجديدة للجريمة المتعلقة بالمستهلك الإلكتروني التي تطورت بشكل لافت، وأصبحت معقدة إلى أبعد مدى، ما يتطلب منا العمل على مكافحتها بصورة فاعلة وفعلية من خلال استصدار قوانين وتنظيمات خاصة تجرم العدوان الذي من شأنه أن يؤثر على صحة وأمن وسلامة المستهلك الإلكتروني. كذا تجريم التعامل في البيانات الشخصية للمستهلك والمتعلقة بالعقود الالكترونية بدون إذن وحماية وسائل الدفع الالكتروني مما يضمن توفير حماية المحتوى ضمان سرية المعلومات.

و تتجلى أهم التوصيات التي يمكن الخروج بها من خلال الدراسة في ما يلي :

في ظل صعوبة الاعتماد على التجارة الالكترونية المستحدثة في الجزائر كبديل عن التجارة الكلاسيكية، خاصة أمام عدم الوعي المجتمعي بأهمية هذا النشاط وكذا التأخر في مجال البنية

التحتية للاتصال خاصة الانترنت، مع عدم إنكار جهود الدولة على توفير مختلف الشروط القانونية والمتطلبات اللازمة لقيام هذا النوع من النشاط، تخلص بالتوصيات والمقترحات الآتية:

توفير الحماية القانونية للمستهلك من أجل ضمان والحفاظ على مصالحه، ووضع تقنين معلوماتي لحماية سائر التصرفات المبرمة عبر الانترنت. بالإضافة إلى تكوين أطر متخصصة في ميدان المعلوماتية والعقود المبرمة عن بعد واستحداث آليات جديدة لوقاية من الأفعال المجرمة في المجال الإلكتروني خاصة عند الحديث عن المستهلك الذي يعتبر الطرف الضعيف في العلاقة التعاقدية.

توعية المستهلكين في البيئة الإلكترونية بحقوقهم عن طريق ندوات وطنية وأيام دراسية يؤطرها المتخصصين، وكذا من الضروري أن يحجم المستهلك الإلكتروني الجزائري على إبرام المعاملات الإلكترونية في مجال التسويق الإلكتروني، إلى غاية خلق تأطير قانوني.

إيجاد طرق عملية وآمنة للتوقيع الإلكتروني وحماية شبكات المعلومات ومواقع الانترنيت الخاصة بمواقع التجارة الالكترونية خاصة من هجمات القرصنة.

الاستفادة من تجارب الدول المتقدمة في مجال التجارة الالكترونية والمعلوماتية والأخذ بخبراتها، وذلك بإقامة علاقات تتعلق بالمجال الالكتروني.

ضرورة حماية المستهلك من عمليات الاحتيال والمواقع الوهمية أو المحتوى غير المشروع للخدمات والمنتجات المعروضة أضحى ضرورة مفروضة على أرض الواقع، فالثقة وحماية المستهلك تحديان يسيران بتوازن مع سائر مراحل أنشطة التجارة الالكترونية، وعلى الدولة أن تضمن هذه الثقة والحماية بإدخال جميع القطاعات الضرورية للعمل على ذلك.

الحماية القانونية للمصنفات الرقمية من جرائم التقليد

Legal protection of digital works against counterfeiting crimes

د. سويلم فضيلة أستاذة محاضرة قسم " أ "
كلية الحقوق و العلوم السياسية.
جامعة د. مولاي الطاهر- سعيدة -الجزائر

مقدمة:

لقد كان للتقدم التكنولوجي الهائل في مجال المعلوماتية و ما أفرزه من تطورات في شتى مجالات الحياة الاقتصادية و الاجتماعية و القانونية، الأثر المباشر على واقع حقوق الملكية الفكرية و تحديداً على حقوق المؤلف[1] التي عرفت ظهور مصنفات فكرية جديدة ذات طبيعة متميزة مرتبطة أساساً باستخدام تقنيات الاتصال والمعلومات الحديثة، اصطلح على تسميتها بالمصنفات الرقمية[2]، حيث فرضت هذه التقنيات الحديثة المتفاعلة في مجال الاتصالات نفسها على حقوق المؤلف المتدفقة عبر شبكة الانترنت، سواء من حيث محلها أو مضمونها، بما توفره من أشكال جديدة للتعبير و الإبداع الفكري، و بما تتيحه من وسائط الكترونية متنوعة.[3]

و في ظل هذا التطور التقني الذي ساهم في تسهيل عملية تداول المصنفات الرقمية و استنساخها بسرعة هائلة، أضحت البيئة الرقمية تشكل مجالاً خصباً لانتهاك حقوق المبدعين و المؤلفين لهذه المصنفات، فتعددت بذلك مظاهر الاعتداء عليها بتعدد الوسائل التقنية الحديثة و بسرعة تطورها، الأمر الذي أدى إلى انتشار أشكال مختلفة من الاعتداءات و من أبرزها جرائم التقليد الالكترونية.

و لما كانت هذه المصنفات باعتبارها مصدراً هاماً للتزود بمختلف المعارف والعلوم و المعلومات، تمثل قيماً مادية واقتصادية هامة، سواء بالنسبة لمؤلفي هذه المصنفات أو الجمهور

---

[1]- تشمل حقوق المؤلف نوعين من المصنفات الفكرية المحمية قانونا و هي : المصنفات الأصلية و المصنفات المشتقة من الأصل.

[2]- سلام منعم مشعل و محمد سمير صالح، الحماية القانونية لحقوق الملكية الفكرية الرقمية، المجلة الأكاديمية للبحث القانوني، المجلد 08، العدد 1، 2017، ص. 105.

[3]- كوثر مازوني، قانون الملكية الفكرية في مواجهة التكنولوجيات الحديثة التجربة الجزائرية، دار هومه، الجزائر، 2016، ص. 37.

المتلقي لها أو الاقتصاد ككل[1]، فإن مسألة حمايتها من مختلف جرائم التقليد، تتطلب لا محالة إيجاد أنظمة قانونية كفيلة بحماية هؤلاء الأطراف، و ملائمة لطبيعتها الرقمية بوصفها وليدة بيئة معلوماتية.

و على إثر هذه التحديات القانونية و التقنية التي تواجه واقع المصنفات الرقمية، يثور التساؤل في هذه الدراسة عن: مدى توافق أحكام الأمر 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة[2] مع الطبيعة الرقمية لهذه المصنفات؟ و إلى أي مدى وفق المشرع الجزائري بمقتضى هذا الأمر في إيجاد الآليات الكفيلة بمكافحة جرائم التقليد الواقعة عليها، مراعياً في ذلك تحقيق التوازن المطلوب بين حماية حقوق مؤلفي هذه المصنفات و بين حقوق مستخدميها؟

إن الإجابة على هذه الإشكالية تستلزم القيام بدراسة وصفية تحليلية لأحكام الأمر 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة، لإبراز ما إذا كانت أحكامه تتسم بالمرونة الكافية و القادرة على حماية هذه المصنفات أم أنها تستدعي بعض التعديل كي تستوعب هذه الإبداعات الحديثة، أم أن الأمر يستلزم استحداث قواعد جديدة تطبق على هذا النوع من المصنفات، كل ذلك بهدف الوصول إلى الحلول المناسبة التي تساهم في تقرير الحماية القانونية لهذه المصنفات في الفضاء الرقمي.

و للإحاطة بالجوانب القانونية لهذه الإشكالية، سيتم بداية تحديد نطاق الحماية القانونية المقررة للمصنفات الرقمية (المبحث الأول)، ثم بيان الآليات التي رصدها المشرع الجزائري لحماية هذه المصنفات من جرائم التقليد.(المبحث الثاني)

المبحث الأول : نطاق الحماية القانونية للمصنفات الرقمية

تعتبر المصنفات الرقمية التي أفرزتها التطورات التكنولوجية الحديثة، ثمرة الإبداع التكنولوجي الناجمة عن اقتران الإبداع البشري بالثورة المعلوماتية التي فجرها اختراع الحاسب الآلي، فالتطور الذي لحقه أدى إلى تغيير جذري في عملية الإبداع التقليدي للمصنفات[3]، من خلال ما أتاحته الشبكة الرقمية من وسائل اتصال حديثة، كل ذلك كان له الأثر الكبير في

[1] - مسعودي يوسف، النظام القانوني لحماية المصنفات الرقمية، دراسات قانونية، المجلد 2، العدد 4، 2009، ص. 113.

[2] - الأمر رقم 03-05 الصادر في 19 جويلية 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، ج.ر.، 23 جويلية 2003، العدد 44.

[3] - سوفالو أمال، حماية الملكية الفكرية في البيئة الرقمية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، جامعة الجزائر 1، 2016-2017، ص. 11.

تغيير الكثير من المفاهيم القانونية في مجال حقوق المؤلف، الأمر الذي ساهم في تغيير مدلول المصنف و في طبيعته المادية بعدما كانت شرط أساسي في حماية المصنفات،[1] (المطلب الأول)

فضلا عن ذلك، ساهم اختلاف طبيعة العالم الافتراضي و خصوصية المعلومات الرقمية، في ظهور أصناف متنوعة من المصنفات التي فرضتها التقنية الرقمية، و كذا في طرح بعض الإشكالات حول كيفية ممارسة مؤلفي هذه المصنفات المستجدة لمختلف الحقوق المخولة لهم، متى ما كانت إبداعاتهم تحظى بالحماية القانونية.(المطلب الثاني)

المطلب الأول: مفهوم المصنفات الرقمية المحمية قانوناً

تعتبر المصنفات الرقمية التي أفرزتها التطورات التكنولوجية الحديثة، مصنفات جديدة تختلف في طبيعتها عن سابقاتها من المصنفات التقليدية سواء من حيث الطابع الإبداعي فيها، أو من حيث طريقة التعبير عنها، الأمر الذي جعلها محل دراسة و اهتمام من قبل الباحثين في مجال الملكية الفكرية بالرغم من حداثة هذا المصطلح محاولين تحديد تعريفها و عناصرها.[2](الفرع الأول)

علاوة على ذلك، تطرح الطبيعة الرقمية لهذه المصنفات الحديثة تساؤلات حول مدى استيفائها للشروط المطلوبة بمقتضى قانون حقوق المؤلف، حتى تمتع بالحماية المقررة للمصنفات الفكرية بوجه عام.(الفرع الثاني)

الفرع الأول: تعريف المصنفات الرقمية

بالرغم من أن المشرع الجزائري لم يورد أي تعريف صريح و مباشر للمصنفات الرقمية بمقتضى الأمر 03-05 سالف الذكر، مكتفياً بإدماج برامج الحاسوب ضمن نطاق المصنفات الأصلية المحمية بموجب هذا الأمر، و بإدراج قواعد البيانات في قائمة المصنفات المشتقة عنها، إلا أنه في مقابل ذلك أقر بوجود هذه المصنفات ضمنياً من خلال النص[3]- في معرض حديثة عن استغلال الحقوق المالية- على إمكانية المؤلف إبلاغ مصنفه إلى الجمهور بأية منظومة معالجة معلوماتية، مما يعني إمكانية بثها و نشرها بالشكل الرقمي.

[1]- محمد حماد مرهج الهيتي، نطاق الحماية الجنائية للمصنفات الرقمية، مجلة الشريعة و القانون، العدد 48، أكتوبر 2011، ص. 369.

[2]- سوفالو أمال، المرجع السابق، ص. 10.

[3]- المادة 27 من الأمر 03-05 سالف الذكر.

هذا فضلا عن عدم حصره لقائمة المصنفات الفكرية المحمية قانوناً الوارد ذكرها في المادة 4 من الأمر 03-05، مما يفسح المجال لإمتداد الحماية القانونية لتشمل المصنفات الرقمية و غيرها من مصنفات أخرى جديدة قد توجدها التطورات التكنولوجية مستقبلا، مهما كان شكلها أو مظهر التعبير عنها.

أما من الناحية الفقهية، فقد عرفها البعض بأنها:" تلك المصنفات الإبداعية العقلية التي تنتمي إلى بيئة تقنية المعلومات، و التي يتم التفاعل معها بشكل رقمي "[1]، و في هذا المضمون أيضا عرفها البعض الآخر بأنها:"كل مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات وفق المفهوم المتطور للأداء التقني ووفق اتجاهات تطور التقنية في المستقبل القريب"[2]، كما عرفها جانب آخر بأنها: "كل نتاج ذهني مبتكر وضع بصيغة رقمية أو تم تحويله من الصيغة الأولية التي هو عليها إلى صيغة رقمية".[3]

يتضح من خلال هذه التعاريف أن المصنفات الرقمية لا تشكل في حقيقتها طائفة جديدة من المصنفات الفكرية المحمية بموجب قانون حقوق المؤلف، و إنما هي فقط طريقة جديدة للتعبير عن المصنفات بشكل رقمي، سواء أكانت هذه المصنفات الرقمية في حقيقتها مصنفات تقليدية و تم تحويلها من صيغتها الأصلية إلى صيغة رقمية دون تعديل أو بعد التعديل فيها، و سواء أكانت هذه المصنفات الرقمية مبتكرة أصلا بالصيغة الرقمية بحيث تم إنشاؤها لأول مرة في البيئة الافتراضية بشكلٍ رقمي.[4]

الفرع الثاني: شروط حماية المصنفات الرقمية

بالنظر للدور الهام الذي تؤديه المصنفات الرقمية في تشجيع البحث العلمي و الإبداع والابتكار، تحظى قوانين حقوق الملكية الفكرية الرقمية بوجه عام بأهمية بالغة في مجال البيئة الرقمية

---

[1]- شعران فاطمة، حماية المصنفات الرقمية في التشريع الجزائري و التشريعات المقارنة، مجلة الدراسات القانونية المقارنة، العدد الثالث، ديسمبر 2016، ص. 110.

[2]- يصرف حاج، الحماية القانونية للمصنفات الرقمية و أثرها على تدفق المعلومات في الدول النامية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص علوم الإعلام و الاتصال، جامعة وهران 1 أحمد بن بلة، 2015-2016، ص. 35.

[3]- سوفالو أمال، المرجع السابق، ص. 15.

[4]- سوفالو أمال، المرجع السابق، ص. 15.

بوصفها ركيزة أساسية لحماية هذه البيئة، من خلال حماية كل إبداع فكري يعرض عبر وسائلها المختلفة متى توافرت شروط الحماية المقررة له.[1]

و استناداً لمضمون أحكام الأمر 03-05 المذكور أعلاه،[2] يتعين على هذه المصنفات حتى تتمتع بالحماية القانونية التي يكفلها هذا الأمر استيفائها لشرطين أساسيين:

الشرط الأول: الأصالة

تعبر المصنفات عن التصاقها و ارتباطها الوثيق بالشخصية الفكرية للمؤلف، باعتبارها وليدة إبداعه الذهني و العقلي[3]، لذا يقتضي شرط الأصالة:" أن يكون المصنف من إنتاج ذهني خالص للمؤلف"، بحيث يبرز من خلاله عن شخصيته، سواء في جوهر الفكرة المعروضة أو في طريقة العرض أو التعبير أو الترتيب أو الأسلوب،[4] فالأصالة تكمن في أشكال التعبير لا في الأفكار وهي غير مقترنة بشرط الجدة.

إن تعريف الأصالة على هذا النحو الذي يركز على شخصية المؤلف أكثر من الجهد الذهني المبذول من جانبه، ينسجم مع العديد من المصنفات الفكرية، إلا أنه لا يتلاءم مع المصنف الرقمي الذي بالرغم من تميزه بالطابع الإبداعي، إلا أنه غالبا ما يتعذر توافر البصمة الشخصية للمؤلف فيه.

و من هنا يتبين أن هذه المصنفات التكنولوجية الحديثة التي اعترف لها المشرع الجزائري بالحماية على أساس حق المؤلف، تثير صعوبة في تطبيق هذا التعريف الشخصي للأصالة عليها، لأنها تمثل مجموعة من القواعد الرياضية أو الفنية أو البيانات التي ينبغي على المؤلف مراعاتها لمنح المصنف المعلوماتي شكله النهائي، و التي يتعذر انطباعها بالبصمة الشخصية لمؤلفها.

و مراعاة لطبيعة هذه المصنفات يمكن تعريف الأصالة بأنها:"الإسهام الذهني للمؤلف"، أو بتعبير آخر هي:"الإبداع أو الابتكار الذي لا يتحقق إلا بواسطة بذل جهد ذهني أو فكري"، وهذا يعني أنه يكفي لتمتع المصنف بالحماية أن يتضمن مجهود ذهني من مؤلفه حتى و إن لم يعكس ذلك بصمته الشخصية، و هذا التعريف الموضوعي يتماشى و طبيعة المصنف الرقمي.

---

[1]- سلام منعم مشعل و محمد سمير صالح، المرجع السابق، ص. 105-106.

[2]- المواد 03 و 05 و 06 و 07 من الأمر 03-05 سالف الذكر.

[3]- شحاتة غريب شلقامي، الحقوق الأدبية للمؤلف في القانون البحريني، مجلة الحقوق، المجلد 6، 2009، ص، 197.

[4]- إبراهيم الخليلي، دراسة مقارنة بين حق المؤلف و الملكية الصناعية من حيث المفهوم و استغلال الحقوق و الانقضاء مؤسسة كنوز الحكمة للنشر و التوزيع، الجزائر، 2018، ص، 16.

الشرط الثاني: تثبيت المصنف على دعامة رقمية

يتطلب هذا الشرط إفراغ الإنتاج الذهني و تجسيده بشكل مادي ملموس تدركه الحواس، حيث يشترط القانون[1] لإضفاء الحماية الخاصة بحق المؤلف على إبداعه الفكري، ضرورة خروجه من مجال الفكر إلى عالم الواقع المحسوس، و ذلك بإفراغه في صورة مادية يظهر من خلالها إلى الوجود أي تثبيته على دعامة مادية أو رقمية، بغض النظر عن شكل و طريقة التعبير عنه، سواء كانت بالكتابة أو بالصوت أو بالرسم أو بالتصوير أو الحركة...إلخ[2]

و بذلك، يكون المشرع الجزائري[3] قد كفل الحماية للتعبير الذي تظهر فيه الأفكار كيفما كان شكله وطريقة تعبيره[4] ودرجة استحقاقه[5] ووجهته[6]، بمجرد إبداع المصنف، سواء أكان المصنف مثبتا بدعامة أو بمنظومة معالجة معلوماتية، أو بأية وسيلة أخرى تسمح بإبلاغه إلى الجمهور.[7]

المطلب الثاني: أنواع المصنفات الرقمية المحمية قانوناً و الحقوق المترتبة عنها

تتنوع المصنفات في المجال الرقمي بحسب مجال استخدامها و بحسب نوع الوسيلة المستعملة لوضعها رقمياً على شبكة الانترنت، و كذا بحسب الوظيفة التي وجدت من أجلها أو الخدمة التي تؤديها إلى عدة أنواع لا حصر لها،(الفرع الأول) و مهما تعددت و اختلفت صور هذه المصنفات الحديثة، فإنها لا تعدو أن تكون في حقيقتها أعمالا إبداعية فكرية أفرزتها التطورات التكنولوجية المتلاحقة، فهل يحق لمؤلفيها متى ما اتسمت بالابتكار و الأصالة الناتجة عنه و تم تثبيتها بدعامة

---

[1]- المادة 07 من الأمر رقم 03-05 الصادر في 19 جويلية 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، سالف الذكر.

[2] - شريقي نسرين، حقوق الملكية الصناعية، حقوق المؤلف و الحقوق المجاورة، حقوق الملكية الصناعية، سلسلة مباحث في القانون، دار بلقيس، 2014، ص. 18.

[3]- المادة 2/03 من الأمر رقم 03-05 سالف الذكر.

[4]- سواء كان مكتوبا أو شفويا أو معبر عنه بأي طريقة أخرى كالصوت أو الحركة أو الصورة.

[5]- يقصد باستحقاق المصنف قيمته الثقافية و العلمية، و هي مسألة لا يقدرها القانون و إنما ترجع لأذواق الجمهور.

[6]- سواء وجه لأغراض تعليمية أو ثقافية أو تجارية أو لصالح المنفعة العامة...

[7] - مسعودي يوسف، المرجع السابق، ص. 119.

رقمية[1]، اكتساب جميع الحقوق المترتبة عنها؟ وكيف يمكن ممارسة هذه الحقوق في ظل خصوصية البيئة الرقمية (الفرع الثاني)

الفرع الأول: أنواع المصنفات الرقمية المحمية قانوناً

تمثل أهم المصنفات الرقمية التي حظيت باهتمام كبير من قبل التشريعات و الباحثين في المجال القانوني في كل من: برامج الحاسوب و قواعد البيانات وكذا أسماء نطاقات أو مواقع الانترنت. [2]

أولا: برامج الحاسوب

تعرف برامج الحاسوب بأنها:" مجموعة التعليمات بأية لغة أو شفرة يكون القصد منها جعل الحاسوب ذو مقدرة على حفظ و ترتيب المعلومات بصورة تؤدي إلى تحقيق نتيجة أو وظيفة أو مهمة معينة"[3]، و سواء اتخذت صورة برامج تشغيل أو برامج تطبيق فإنها تعد بمثابة الكيان المعنوي لنظام الكمبيوتر.[4]

تعتبر برامج الحاسوب أولى و أهم المصنفات المعلوماتية التي عرفت اهتمام غالبية التشريعات، بما في ذلك المشرع الجزائري الذي حرص على حمايتها بمقتضى الأمر 03-05، نظرا لما تتطلبه من إطارات بشرية مؤهلة تأهيلاً فنياً وتقنيا ًفي هذا المجال، و لإمكانية نشرها وتسويقها بسهولة عبر شبكة الانترنت مع ما تتيحه من طرق وأساليب للتعدي على حقوق مؤلفيها و من بينها طرق التقليد. [5]

ثانيا: قواعد البيانات

قواعد البيانات هي عبارة عن: " مجموعة من البيانات المرتبة والمنظمة ترتبط فيما بينها بروابط منطقية، و يمكن من خلال هذه التقنية حفظ وتعديل وحذف المعلومات بطرق سلسة، كما تتيح استخراج البيانات المحفوظة و استرجاعها"، أو بمعنى آخر هي: ":" مجموعة من البيانات

---

[1]- هنية شريف، تأثير المعلوماتية على عقود استغلال حق المؤلف، حوليات جامعة الجزائر 1، العدد 29، الجزء الثاني، ص. 21.

[2]- يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة إلى الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي من 2 إلى 4 جويلية 2002، النادي العربي للمعلومات، دمشق، سوريا، 2002، ص. 11.

[3] - جدي نجاة، المعلوماتية و حقوق المؤلف، مجلة دراسات و أبحاث، العدد 6، 2012، ص. 189.

[4] - زيجة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، الجزائر، 2011، ص. 87.

[5]- يصرف حاج، المرجع السابق، ص. 36.

والمعلومات المخزنة بترتيب ونسق إلكتروني معين يسهل التعامل معها وحفظها واسترجاعها واستخراج النتائج منها".[1]

تعتبر قواعد البيانات أحد أنواع المصنفات الرقمية المرتبطة بالكمبيوتر و بالتطورات التكنولوجية، و قد اعترف لها المشرع الجزائري[2] صراحة بالحماية القانونية مهما كان شكلها لكونها تمثل ابتكارات فكرية تستمد أصالتها من انتقاء موادها (محتواها) أو ترتيبها، سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة - أي كانت في شكل مقروء آلياً - أو بأي شكل من الأشكال الأخرى.[3]

وقد ساهم الانتشار الواسع لشبكة الإنترنت و تطور الاتصالات وتبادل المعلومات إلى تطور هذه التقنية، فبعدما كانت تحصر في قواعد تخزين و نقل للمعلومات و البحث عنها داخل أنظمة الكومبيوتر أو عبر وسائط مادية تحتويها، تحولت إلى مخازن للمعلومات تتيح للمستخدم معالجتها و البحث في محتواها و الاستفادة منها بطريقة آلية[4]، فظهرت بذلك قواعد البيانات على الخط كمفهوم متطور لهذه التقنية.

ثالثا: مواقع الانترنت

يتكون محتوى مواقع الانترنت من: "مجموع من المكونات الرقمية المتمثلة في برامج خاصة بابتكار الموقع (إدارته) و برامج الخدمة"، و هي تعتبر من أهم وسائل التواصل عبر الانترنت، نظرا لما تحتويه من معلومات و بيانات رقمية قد تأخذ شكل صور أو أصوات أو رسوم أو نصوص معلومات أو فيديو، و التي تسمح لمستخدم شبكة الانترنت من الإبحار في العالم الافتراضي.[5]

و من أهم مكونات مواقع الانترنت أسماء النطاق و هي:" عبارة عن سلسلة أحرف و/أو أرقام مقيّسة و مسجلة لدى السجل الوطني لأسماء النطاق، و التي تسمح بالتعرف و الولوج إلى

---

[1]- سهام بنت سلمان الجريوي، البحث في قواعد البيانات، دراسات، مجلة المعرفة، 18 ماي 2016، تم الاطلاع عليه يوم 05 مارس 2020 على الساعة 19 مساءً، في الموقع: http://www.almarefh.net/show_content_sub.php?SubModel=141&ID=2721

[2] - المادة 5 من الأمر رقم 03-05 سالف الذكر.

[3] - خالدة هناء سيدهم، حماية حقوق الملكية الفكرية للمصنفات الرقمية في بيئة الانترنت، أعمال المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، طرابلس، لبنان، 24 و 25 مارس 2017، كتاب أعمال المؤتمرات دورية دولية محكمة تصدر فصليا عن مركز جيل البحث العلمي، 2017، ص. 37.

[4]- سهام بنت سلمان الجريوي، المرجع السابق.

[5]- يصرف حاج، المرجع السابق، ص. 39.

الموقع الالكتروني"[1]، و تظهر أهمية إسم النطاق من خلال الوظيفة التي يؤديها على شبكة الانترنت، و المتمثلة في تسهيل الدخول لمستخدمي هذه الشبكة إلى المواقع الالكترونية للاستفادة من المعلومات و الخدمات التي تقدمها، سواء كانت علمية أو تجارية...إلخ[2]

تعتبر مواقع الانترنت أحد أهم المصنفات الرقمية الناشئة في بيئة الانترنت، و مع ذلك لم تحظى بالحماية في ظل التشريع الجزائري خاصة و أنها تثير عدة إشكالات قانونية تحتاج إلى تنظيمها و المتعلقة بمسألة تطابق عنوان موقع الانترنت مع اسم تجاري أو علامة تجارية، و كذا التكييف القانوني لمحتواها الذي يتضمن مزيج من مختلف المعلومات بل وحتى مصنفات أخرى كبرامج الحاسوب و قواعد البيانات على الخط. [3]

الفرع الثاني: الحقوق المترتبة عن المصنفات الرقمية

بتوافر شرطي الأصالة و التثبيت بدعامة رقمية يمنح للمصنف الرقمي الحماية القانونية، و يتمتع مؤلفه بحقوق معنوية[4] و أخرى مادية، و تمثل حقوقه المعنوية[5] في :

- حق المؤلف في الكشف عن مصنفه الرقمي و إخراجه للعلن عن طريق عرضه أو نشره بعد ترقيمه عبر وسائل الشبكة المعلوماتية و التي تسمح بطبيعتها بسهولة العرض و التوزيع لهذا المصنف، و بتحقق العلانية.
- الحق في نسب المصنف إليه إلكترونياً من خلال تسجيل كل المعلومات المتعلقة بهويته (كاسمه العائلي أو اسم مستعار) و شخصيته و أصحاب الحقوق داخل النسخة الرقمية للمصنف، و يعد ذلك بمثابة حماية للمصنف في نسخته الأصلية، لأن النسخ المقلدة لا تحتوي على تلك المعلومات.
- الحق في سحب المصنف الرقمي من التداول عبر شبكة الانترنت: متى رأى المؤلف أن مصنفه لم يعد مطابقا لقناعاته، و قد يطلب وقف بثه أو نشره لإجراء التعديلات التي

---

[1]- المادة 8/06 من القانون 18-05 المؤرخ في 10 ماي 2018 يتعلق بالتجارة الالكترونية ، ج.ر. 16 ماي 2018، العدد 28.

[2]- يصرف حاج، المرجع السابق، ص. 39.

[3] - مسعودي يوسف، المرجع السابق، ص. 116.

[4] - المادة 21 من الأمر رقم 03-05 سابق الذكر.

[5] - المواد من 22 إلى 26 من الأمر رقم 03-05 سالف الذكر.

يراها مناسبة عليه، غير أنه لا يمارس المؤلف هذا الحق إلا بعد دفع تعويض عادل عن الأضرار التي يلحقها عمله هذا بمستفيدي الحقوق المتنازل عنها. [1]

- الحق في احترام سلامة المصنف و منع التحوير والدمج الرقمي له: من خلال الاعتراض على أي تعديل أو تشويه أو تحريفا لمصنفه أو المساس بسمعته، فتحوير المصنف من صورته العادية إلى الصورة الرقمية ليتلاءم مع تقنيات الدمج التي توفرها المنتجات الرقمية الحديثة دون موافقة المؤلف يمثل اعتداء على حقه الأدبي في احترام سلامة مصنفه.[2]

أما حقوقه المادية[3] التي يمارسها للحصول على عائد مالي فتشمل ما يلي:

- الحق في استنساخ المصنف[4] في عدة نسخ و إيصاله للجمهور بأي طريقة أو شكل سواء كان بصورة مؤقتة أو دائمة، بما في ذلك التصوير الفوتوغرافي، أو السينمائي، أو التسجيل الرقمي الإلكتروني...إلخ [5]
- الحق في إبلاغ المصنف الرقمي إلى الجمهور من خلال عرضه و وضعه حيز التداول بأية وسيلة من وسائل الاتصال المعلوماتية أو الرقمية.
- الحق في تحويل المصنف كترجمته أو اقتباسه أو إعادة توزيعه، و غيرها من التحويلات المدخلة على المصنف، و التي يتولد عنها مصنفات مشتقة من الأصل.[6]

---

[1] - المادة 24 من الأمر رقم 03-05 سابق الذكر.

[2] - أسامة بدر، بعض مشكلات تداول المصنفات عبر الانترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص. 63.

[3] - المادتين 27 و 28 من الأمر رقم 03-05 المذكور أعلاه.

[4] - استثناءًا يسقط هذا الحق في ثلاث حالات محددة قانونا تشمل : نقل المصنف لغرض خاص (المادة 41 من الأمر 03-05) و نقل المصنف لغرض عام (المادة 42 من نفس الأمر)، و كذا نقله المصنف من قبل أجهزة الإعلام (المواد من 45 إلى 51 من ذات الأمر).

[5] - فاطمة الزهراء بلحسين و طارق مالكي، حقوق المؤلف وحماية مصنفاته الرقمية في شبكة الانترنت، عدد خاص بالمؤتمر الدولي المحكم حول الملكية الفكرية على المؤلفات، طرابلس، لبنان، 27 و 28 مارس 2020، سلسلة كتاب أعمال المؤتمرات دورية دولية محكمة تصدر فصليا عن مركز جيل البحث العلمي، العام الثامن، العدد 27، مارس 2020، ص. 72.

[6] - فاضلي إدريس، المدخل إلى الملكية الفكرية، الملكية الأدبية و الفنية و الصناعية، ديوان المطبوعات الجامعية، 2007، ص. 122.

- حق التتبع للحصول على نسبة مئوية من ثمن بيع أو إعادة بيع مصنفه الأصلي، و تقدر نسبة مشاركة المؤلف بـ 05% من مبلغ بيع أو إعادة بيع المصنف، لكن هذا الحق خاص فقط بمصنفات الفنون التشكيلية.[1].

المبحث الثاني : آليات الحماية القانونية للمصنفات الرقمية من جرائم التقليد

لقد كرس المشرع الجزائري بمقتضى المواد من 143 إلى 160 من الأمر 03-05 سابق الذكر عدة آليات تكفل الحماية لأصحاب الحقوق على المصنفات الرقمية، و التي تسمح لمؤلف هذه الإبداعات الرقمية الذي اعتدى على حقوقه المادية أو الأدبية بالتقليد، بمواجهة الانتهاكات الواقعة على حقوقه، كما تتيح له المطالبة بالتعويض على أساس المسؤولية المدنية. (المطلب الأول)

و نظرا للأهمية التي تحظى بها هذه المصنفات لم يكتفي المشرع فقط بالتدابير التحفظية والدعوى المدنية لحمايتها، بل أضاف أيضا **آليات أكثر قوة و ردع تتمثل في الحماية الجنائية، بغية ضمان عدم تعرض مرتكبي أفعال التقليد لحقوق أصحاب** هذه المصنفات **المنشورة عبر شبكة الإنترنت.** (المطلب الثاني)

المطلب الأول: آليات الحماية المدنية للمصنفات الرقمية من جرائم التقليد

طبقا لأحكام الأمر 03-05 يحق لمؤلف هذه الإبداعات الرقمية الذي اعتدى على حقوقه المادية أو الأدبية، متى كان صاحب صفة و مصلحة في طلب الحماية التحفظية، اتخاذ الإجراءات التحفظية اللازمة لوقف التعدي على هذه المصنفات و منع تداولها (الفرع الأول)، بالإضافة إلى ذلك، يحق له المطالبة بالتعويض عن الضرر المادي أو المعنوي الذي لحق بمصنفاته أو بسمعته نتيجة ارتكاب أفعال التقليد المحظورة قانوناً.(الفرع الثاني)

الفرع الأول: التدابير التحفظية المتخذة في مواجهة جرائم تقليد المصنفات الرقمية

يحق للمؤلف مالك الحقوق المتضرر من أفعال التقليد، أن يطلب من الجهة القضائية المختصة اتخاذ التدابير التحفظية اللازمة لمنع الاعتداء الوشيك الوقوع على حقوقه أو لوضع حد لهذا المساس المعاين، هذا فضلا عن حقه في طلب التعويض الأضرار التي لحقت به من جراء أفعال التقليد.[2]

تهدف هذه الإجراءات ذات الطابع الاستعجالي إلى مواجهة اعتداءات التقليد التي لحقت فعلاً بالمصنف بغرض وضع حد سريع لها لحين فصل المحكمة في النزاع المعروض، و يتم

---

[1]- شريقي نسرين، المرجع السابق، ص. 48.

[2] - المادة 144 من الأمر رقم 03-05 سالف الذكر.

ذلك من خلال حصر الأضرار المترتبة ثم اتخاذ التدابير اللازمة لإزالتها و المحافظة على حقوق المؤلف.[1]

و تمثل هذه التدابير التحفظية التي يأمر باتخاذها رئيس المحكمة المختصة بناء على طلب المؤلف المتضرر أو ممثله فيما يلي:

- إيقاف كل عملية صنع جارية ترمي إلى الاستنساخ غير المشروع للمصنف المحمي أو تسويق دعائم مصنوعة بما يخالف حقوق مؤلفيه: و ذلك بهدف وقف الاعتداء على المصنف المحمي و منع المعتدي من إعادة نسخ المصنفات المقلدة أو من تداولها بين الجمهور.
- حجز دعائم المصنفات المقلدة و الإيرادات المتولدة عن الاستغلال غير المشروع لهذه المصنفات.
- حجز كل عتاد مستخدم لصنع الدعائم المقلدة.

كما يمكن لرئيس المحكمة أن يأمر بدفع كفالة من قبل المدعي مقابل اتخاذ هذه الإجراءات.[2]

و يتولى القيام بالتدابير التحفظية ضباط الشرطة القضائية أو الأعوان المحلفين التابعين للديوان الوطني لحقوق المؤلف والحقوق المجاورة الذين يحق لهم معاينة إعتداءات التقليد الماسة بحقوق المؤلف، باعتبارهم الأشخاص المؤهلون قانونا بذلك، كما يجوز لهم القيام بصفة تحفظية بحجز نسخ دعائم المصنفات المقلدة شريطة وضعها تحت حراسة الديوان، على أن يتم إخطار رئيس المحكمة فورا عن هذا الحجز بناء على محضر مؤرخ و موقع قانوناً يثبت النسخ المقلدة المحجوزة، ويتم الفصل في طلب الحجز التحفظي في أجل 03 أيام على الأكثر من تاريخ الإخطار.[3]

في مقابل ذلك، يمكن للمدعي عليه (مرتكب التقليد) الذي يدعي التضرر من التدابير التحفظية المذكورة أعلاه الاعتراض عليها بأن يطلب من رئيس المحكمة المختص في القضايا الإستعجالية خلال ثلاثون يوما من تاريخ صدور هذه التدابير، رفع اليد أو خفض الحجز أو حصره

---

[1] - إدريس الفاخوري، طرق و وسائل حماية حقوق المؤلف، مجلة عدالة للدراسات القانونية و القضائية، دار السلام للطباعة و النشر، الطبعة الأولى، الرباط، المغرب، 2019، ص. 17.

[2] - المادة 147 من الأمر رقم 03-05 سالف الذكر.

[3] - المادة 146 من الأمر رقم 03-05 سالف الذكر.

أو رفع التدابير التحفظية الأخرى، مقابل إيداع مبالغ مالية كافية لتعويض مالك الحق في حالة ما إذا كانت دعواه مؤسسة.[1]

إذا كانت الإجراءات التحفظية سابقة على رفع الدعوى المدنية يجب أن ترفع في أجل ثلاثون يوما من صدور الأمر بالحجز التحفظي، و في غياب هذه الدعوى يمكن لرئيس المحكمة المختص في القضايا الإستعجالية أن يأمر بناء على طلب الطرف (مرتكب التقليد) الذي يدعي التضرر من تلك التدابير، برفع اليد عن الحجز أو رفع التدابير التحفظية الأخرى[2]، أما إذا كانت موازية لها ففي هذه الحالة يبقى الإجراء التحفظي ساريا إلى غاية الفصل في دعوى الموضوع.[3]

يستخلص مما سبق، أن المشرع الجزائري قد منح للمؤلف مجموعة من الإجراءات كوسيلة تحفظية لضمان وقف الاعتداء على حقوقه والحد من تفاقم الأضرار الناجمة عنه، غير أن هذه التدابير التحفظية التي أقرها المشرع لفائدة المؤلف[4] المتضرر من تقليد مصنفه الرقمي، لا تشكل شرطاً لقبول الدعوى المدنية أو الجزائية إذ يمكن التقاضي دون المطالبة بها، و مع ذلك يجوز استخدام محاضر الحجز التحفظي كأدلة لإثبات المسؤولية أمام القضاء المدني أو الجزائي.[5]

الفرع الثاني: دعوى التعويض عن جرائم تقليد المصنفات الرقمية

بعد استنفاذ الإجراءات التحفظية سالفة الذكر، يمكن للمؤلف المتضرر المطالبة بالتعويض لجبر الضرر الذي لحق به، و تستند دعوى التعويض عن **جرائم تقليد** المصنفات الرقمية في القانون

[1] - المادة 148 من الأمر رقم 03-05 سالف الذكر.

[2] - المادة 149 من الأمر رقم 03-05 سابق الذكر.

[3]- **حاج صدوق لبندة، الحماية القانونية للمصنفات الفكرية وفقا للتشريع الجزائري**، عدد خاص بالمؤتمر الدولي المحكم حول الملكية الفكرية على المؤلفات، طرابلس، لبنان، 27 و 28 مارس 2020، سلسلة كتاب أعمال المؤتمرات دورية دولية محكمة تصدر فصليا عن مركز جيل البحث العلمي، العام الثامن، العدد 27، مارس 2020، ص. **24**.

[4]- يمكن أيضا للمؤلف اتخاذ إجراء وقائي آخر يتمثل في الإيداع القانوني لمصنفه الرقمي، من خلال تسليم نسخة منه أو أكثر للجهة الرسمية المختصة بالإيداع قانونا، و يعتبر هذا الإجراء من أهم إجراءات حماية حقوق المؤلفين على مصنفاتهم.

[5]- بوراوي أحمد، الحماية القانونية لحق المؤلف و الحقوق المجاورة في التشريع الجزائري و الاتفاقيات الدولية، أطروحة مقدمة لنيل درجة دكتوراه العلوم في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة باتنة 1، 2014-2015، ص. 274-275.

الجزائري إلى نص المادتين 143 و 144 من الأمر 03-05 المذكور أعلاه، و ذلك متى ما توافرت شروط هذه الدعوى القائمة على أساس المسؤولية المدنية.[1]

أولا: شروط دعوى التعويض

استنادا إلى نص المادة 143 من الأمر 03-05 المذكور أعلاه، تكون الدعوى القضائية لتعويض الضرر الناتج عن الاستغلال غير المرخص به لمصنف المؤلف و الأداء لمالك الحقوق المجاورة من اختصاص القضاء المدني.[2]

يشترط لقبول دعوى التعويض من الناحية الموضوعية، نفس العناصر التي يتطلبها القانون المدني لقيام المسؤولية التقصيرية[3]، و المتمثلة في وجود خطأ (أفعال التقليد)، و وجود ضرر مترتب عنه، وأخيرا علاقة السببية بين أفعال التقليد وإلحاق الضرر بالمؤلف.

و عليه، يجب على المدعي المؤلف إثبات ارتكاب الخطأ من قبل المعتدي، أي إثبات وجود استغلال غير مشروع قام به المدعى عليه لمصنفه المحمي قانونا و المتمثل في أحد صور التقليد الوارد ذكرها في الأمر 03-05، ويتم إثبات ذلك بكافة طرق الإثبات.

كما يشترط إثبات الضرر الذي لحق به من جراء هذه الأفعال غير المشروعة التي قام بها المعتدي سواء كان ضرر مادي أو معنوي، و كذا إثبات العلاقة السببية بينهما من خلال إثبات أن أفعال التقليد هي السبب المباشر في حدوث الضرر و إلا انعدمت المسؤولية، وتخضع هذه الشروط في تقديرها للسلطة التقديرية للقاضي للتأكد من مدى توافرها.[4]

تجدر الملاحظة إلى أن حماية أي مصنف توجب على مدعي الاعتداء إثبات أنه المالك الحقيقي و القانوني لحقوق المؤلف على هذا المصنف، سواء تعلق الأمر بالدعوى المدنية أو

---

[1]- **تطبق قواعد المسؤولية العقدية إذا كان الاعتداء على حق المؤلف قد صدر من شخص تربطه بالمؤلف رابطة عقدية، أما إذا كان الاعتداء صادر من الغير الذي لا تربطه بالمؤلف أية علاقة عقدية، فهنا تطبق قواعد المسؤولية التقصيرية.**

[2] - بالنسبة للاختصاص المحلي فحسب المادة 42 من القانون 08-09 المؤرخ في 25 فبراير 2008 المتضمن قانون الإجراءات المدنية و الإدارية ج.ر. 23 أفريل 2008، العدد 21، تعود منازعات حقوق المؤلف إلى اختصاص محكمة مقر المجلس القضائي الموجود في دائرة اختصاصه موطن المدعي عليه، مع العلم أن المشرع قد أحالها إلى الأقطاب القضائية المتخصصة، عملا بأحكام الفقرة الثانية من المادة 32 من نفس القانون.

[3] - المادة 124 من الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني المعدل و المتمم : "كل فعل أيا كان يرتكبه الشخص بخطئه ويسبب ضررا للغير، يلزم من كان سببا في حدوثه بالتعويض ".

[4]- **حاج صدوق ليندة، المرجع السابق، ص. 23.**

بالطلبات المستعجلة في إطار التدابير التحفظية، و عليه يعد شرط ثبوت تملك الحق المعنوي أو حق الاستغلال المالي للمدعي على مصنفه، أساس قبول دعوى التعويض بوصفه شرط يثبت توافر الصفة و المصلحة لدى المدعي في آن واحد.[1]

ثانيا: الجزاءات المدنية المقررة لجرائم تقليد المصنفات الرقمية

يتمثل الجزاء المدني المترتب عن هذه الدعوى في التعويض، و يهدف هذا الأخير إلى جبر و إصلاح الأضرار المترتبة مباشرة عن وقوع التقليد على المصنف الرقمي، سواء تمثلت الأضرار في خسارة مادية أو معنوية أو في تفويت الفرصة، و يخضع تقدير هذا التعويض للسلطة التقديرية للقاضي الذي يستعين بالخبرة للقيام بذلك.

و يتعين على القاضي وفقا لأحكام القانون المدني[2]، تقدير التعويض حسب جسامة الضرر اللاحق بالمضرور دون جسامة الخطأ، وفق معيار ذاتي آخذاً بعين الاعتبار ظروفه الملابسة أي الشخصية، كالظروف الصحية و العائلية و المالية...، على أن يشمل التعويض الخسارة المادية والمعنوية و تفويت الفرصة، بشرط أن يكون نتيجة طبيعية و مباشرة للاستغلال غير المرخص به للمصنف.[3]

و يتم تقدير التعويض حسب المادة 132 من القانون المدني إما نقداً فيدفع كاملا للمضرور أو في شكل أقساط أو في صورة مرتب مدى الحياة، و إما عيناً من خلال إعادة الحالة إلى ما كانت عليه قبل وقوع التعدي.

المطلب الثاني: آليات الحماية الجزائية للمصنفات الرقمية من جرائم التقليد

في مقابل المزايا التي حققتها التكنولوجيا الحديثة و ظهور الانترنت للمصنفات الرقمية و التي أصبحت بفضلها متاحة لمستخدمي هذه الشبكة للاطلاع على هذه المصنفات و اقتناؤها بكل سهولة، انتشرت و تنوعت صور التقليد الواقعة على هذه المصنفات و الماسة بحقوق مؤلفيها سواء من جانبها المادي أو المعنوي[4]، لذا حرص المشرع الجزائري على التصدي لها بموجب المواد من 151 إلى 160 من الأمر 03-05 التي جرم من خلالها مجموعة من الأفعال المكونة لجرائم التقليد.(الفرع الأول)

---

[1]- يونس عرب، المرجع السابق، ص. 30.

[2] - المادة 131 من القانون المدني.

[3] - المادتين 182 و 182 مكرر من القانون المدني.

[4]- كوثر مازوني، المرجع السابق ص. 49-50.

و في سبيل تقرير حماية جنائية فعالة، أقر المشرع الجزائري بمقتضى هذه النصوص - لاسيما في حالة عدم فعالية الإجراءات التحفظية سالفة الذكر في وقف الاعتداء- بتوقيع جملة من الجزاءات المقررة لردع مرتكبي هذه الجرائم في حالة ثبوت مسؤوليهم الجزائية.[1] (الفرع الثاني)

الفرع الأول: جرائم التقليد و صورها

يمثل التقليد أهم صور الاعتداءات التي يمكن أن تقع على حقوق مؤلفي المصنفات الفكرية التقليدية، بل و حتى المصنفات الحديثة التي عرفها العالم الافتراضي في ظل التكنولوجيا الحديثة، و الذي أصبح يطلق عليه وصف "التقليد على الخط" نظرا لطبيعة المعلومات و المصنفات المنشورة رقمياً،[2] كل ذلك يبرز أهمية تعريف جريمة التقليد الواقعة على هذه المصنفات التي تشكل خرقاً لقانون حقوق المؤلف.(أولا)

و طالما أن المشرع الجزائري قد أدمج تطبيقات الحاسب الآلي ضمن قائمة المصنفات المحمية بموجب الأمر 03-05، و اعترف بالمصنفات التي تبث عبر شبكات الاتصال الرقمية متى توافرت فيها شروط الحماية، **فإن أي اعتداء مباشر يقع على الحق المالي أو الأدبي لمؤلفي هذه المصنفات يشكل فعلاً من أفعال التقليد.**[3] (ثانيا)

علاوة على ذلك، حظر المشرع الجزائري **مجموعة من التصرفات التي يكون محلها مصنفات مقلدة، حيث اعتبرها أفعال تقليد** بوصفها تمثل اعتداء بصورة غير مباشرة على الحقوق المالية لمؤلفي المصنفات الأصلية، و يطلق على هذه التصرفات "جرائم التعامل في المصنفات المقلدة".(ثالثا)

أولا: تعريف جنحة التقليد

يقصد بالتقليد عموماً : "نقل شيء عن الأصل و استنساخه كلياً أو جزئياً بصورة احتيالية و تدليسية قصد التحريف و الغش ونسبه لغير صاحبه الأصلي، بهدف إيقاع الغير في الخطأ والخلط بين الشيئين الأصلي و المقلد"، فإذا كان هذا الاستنساخ كليا سمي بالتقليد الحرفي أو المحض، والتقليد بهذه الصورة يمثل اعتداء صارخا لأنه بمثابة سرقة، أما إذا كان جزئيا فيطلق

---

[1] - فاطمة الزهراء بلحسين و طارق مالكي، المرجع السابق، ص. 79.

[2]- كوثر مازوني، المرجع السابق ص. 84-85.

[3]- خالد دوادي، الجريمة المعلوماتية، دار الإعصار العلمي، الطبعة الأولى، عمان، الأردن، 2018، ص. 95.

عليه بالتقليد الجزئي، و العبرة في تقدير هذا التقليد تكون بأوجه الشبه بين الشيء المقلد والشيء الأصلي في أجزائه الرئيسية و الذي من شأنه خداع الجمهور".[1]

و على هذا النحو، يعتبر تقليداً في مجال حقوق المؤلف:" محاكاة مصنف أو إنتاج نُسَخْ على مثاله، سواء كان النسخ كلياً بحيث يبدو المصنف عند تسويقه كالأصل، أو جزئياً متى كانت المحاكـاة تتعلق بأجزائه الرئيسية"،[2] دون ترخيص من أصحاب الحقوق عليه.

لم يتعرض المشرع الجزائري لتعريف جنحة التقليد الواقعة على حقوق المؤلف، مكتفياً بتعداد الأفعال و السلوكات المادية المشكلة للجرائم الموصوفة بالتقليد، أما على الصعيد الفقهي فقد عرفها البعض بأنها:" نقل مصنف لم يسقط في الملك العام من غير إذن مؤلفه"[3]، كما عرفها البعض الآخر بأنها:" كل اعتداء مباشر أو غير مباشر على حقوق المؤلف في

المصنفات الواجب حمايتها أياً كانت طريقة الاعتداء أو صورته"، و في نفس المضمون أيضا عرفها جانب آخر بأنها :" كل اعتداء على حقوق المؤلف و الحقوق المجاورة عن طريق القيام بنشر أو استغلال المصنف...أو عرضه أو بيعه دون إذن المؤلف أو خلفه".[4]

و عليه، يمكن القول بأن جنحة التقليد في نظر الفقه تشمل:" كل إعتداء كلي أو جزئي يمس بالحقوق المعنوية أو المادية لمؤلفي المصنفات المحمية قانوناً أو أصحاب الحقوق عليها[5]، مهما كانت الوسيلة المستعملة، مخالفا بذلك القوانين المتعلقة بهذه الحقوق".[6]

ثانيا: الأفعال المكونة لجنحة التقليد

[1] - زواني نادية، الاعتداء على حق الملكية الفكرية، التقليد والقرصنة، مذكرة لنيل شهادة الماجستير، تخصص الملكية الفكرية، كلية الحقوق و العلوم الإدارية، جامعة الجزائر، 2002-2003، ص. 9- 10.

[2] - عفيفي كمال عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقيقية، لبنان، 2003، ص. 95.

[3] - بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون حقوق المؤلف الجديد الأمر رقم 03-05، دار الخلدونية، الطبعة الأولى، الجزائر، 2007، ص. 76-77.

[4] - بن حليمة ليلى، جنحة التقليد في التشريع الجزائري و التشريع الأردني – دراسة مقارنة -، مجلة آفاق للعلوم، العدد 8، الجزء الأول، جوان 2017، ص. 121 - 122.

[5] - حسب المادة 160 من الأمر 03-05 يحق لكل من المؤلف أو ورثته أو المتنازل لهم عن حقوقه المالية أو ممثله كالديوان الوطني لحقوق المؤلف و الحقوق المجاورة (المادة 132)، تحريك الدعوى العمومية من خلال تقديم شكوى أمام الجهات القضائية المختصة ضد كل من يرتكب أحد أفعال التقليد المجرمة في الأمر 03-05.

[6] - إدريس الفاخوري، المرجع السابق، ص. 33.

لقد كيَّف المشرع الجزائري الأفعال المنصوص عليها في المواد 151 و 152 و 155 من الأمر 03-05 على أنها جنحة التقليد، و حدد بموجبها السلوكيات المادية التي تشكل الركن المادي لها **بوصفها اعتداء على حقوق المؤلفين أو أصحاب الحقوق عليها سواء المعنوية منها أو المادية حتى لو ارتكبت في البيئة الرقمية، و تمثل هذه الأفعال فيما يلي:**

النوع الأول: التقليد المتعلق بالحقوق المعنوية لمؤلف المصنفات الرقمية

و يشمل هذا النوع من التقليد الصور التالية:

1- **الكشف غير المشروع للمصنف الرقمي**: كالقيام بنشر و طرح المصنف الرقمي المتمتع بالحماية القانونية للتداول عبر شبكة الانترنت دون ترخيص من مؤلفه صاحب الحق الاستئثاري بذلك، أو بطريقة مخالفة لما رُخِص بها[1] ، أو القيام بحذف اسم المؤلف وتغييره باسم آخر أو ترك المصنف مجهول الهوية، فكل ذلك يشكل تقليداً لهذا المصنف.

2- **المساس بسلامة المصنف الرقمي**: غالبا ما يتعرض المصنف عند عملية ترقيمه لنشره عبر الانترنت لقدر من المعالجة الفنية والترتيب والتعديل التي قد لا تسمح بالحفاظ على سلامة المصنف بالصورة التي يريدها المؤلف، لاسيما عملية الترقيم في صورتها التفاعلية التي من خلالها يتم إظهار المصنف في شكل جديد وفق صورة معدلة لبثه عبر الانترنت، عن طريق تدخل التقنيات الحديثة بتعديل الأصوات أو بإضافة صورة جديدة[2]، وهو ما يتعارض مع حق المؤلف في احترام سلامة مصنفه، لذا يجب للقيام بهذه العملية الحصول على رخيص منه، و إلا عد ذلك تقليداً.

النوع الثاني: التقليد المتعلق بالحقوق المالية لمؤلف المصنفات الرقمية

يمثل هذا التقليد في:

1- **الاستنساخ غير المشروع للمصنف الرقمي**: بأي أسلوب من الأساليب و بأي شكل من أشكال الاستنساخ في صور نسخ مقلدة، و هذا الصنف من جرائم التقليد هو الأكثر شيوعا في المجال المعلوماتي، كما في حالة تجاوز الناشر عدد النسخ المتفق عليها في العقد،

---

[1]- شعران فاطمة، المرجع السابق، ص. 120.

[2]- مروى أبو العلا، المصنفات الرقمية واستغلالها عبر الانترنت، بحث ودراسة مقارنة، 16 ديسمبر 2017، تم الاطلاع عليه يوم 09 مارس 2020 على الساعة 22 مساءً، في الموقع: المصنفات-الرقمية-واستغلالها-عبر-الان/ https://www.mohamah.net/law

و كذا حالة نشره لمصنف غير مرخص له بذلك أو كان محل سحب من النشر من قبل المؤلف و مع ذلك تعمد الناشر مواصلة عملية النشر بدون ترخيص من مؤلفه، و كذلك السرقة الأدبية تعد أيضا بمثابة جنحة تقليد[1]، استثناء من ذلك، يجوز استنساخ نسخة واحدة من برامج الحاسوب في حالتين:

الحالة الأولى: استعمال برنامج الحاسوب للغرض الذي اكتسب من أجله ووفقا للشروط التي كانت قائمة عند اكتسابه.

الحالة الثانية: تعويض نسخة مشروعة الحيازة من البرنامج بغرض التوثيق في حالة ضياعه، تلفه أو عدم صلاحيته للاستعمال.[2]

-2 **إبلاغ المصنف الرقمي المقلد للجمهور عن طريق أي نظام للمعالجة الآلية**: و ذلك من خلال القيام بنشر أو بث نسخ مقلدة من مصنف أدبي أو فني أو تسجيل صوتي أو برنامج إذاعي سمعي أو سمعي بصري أو أي مصنف آخر، باستخدام تقنيات الاتصال والمعلومات الحديثة.[3]

3- الرفض العمدي لدفع المكافأة المستحقة للمؤلف:

أضاف الأمر 03-05 بمقتضى المادة 155 منه فعلاً آخر يشكل الركن المادي في جنحة التقليد، يتمثل في رفض الشخص الذي رخص له بالاستغلال المادي للمصنف دفع المكافأة المستحقة لمؤلفه عمداً، معتبراً إياه انتهاك للحقوق المحمية بموجب هذا الأمر.[4]

و تعتبر جنحة التقليد بصورها المذكورة أعلاه من الجرائم العمدية التي يلزم لقيامها توافر القصد الجنائي بعنصريه العلم و الإرادة، أي علم الجاني بأنه سلوكه الإجرامي المتمثل في التقليد يرد على الحقوق المادية أو المعنوية لمصنف رقمي ينسب لشخص آخر، سواء من خلال قيامه بنشر هذا المصنف أو المساس بسلامته أو استنساخه أو إبلاغه للجمهور دون وجه حق، و مع ذلك تتجه إرادته إلى القيام بهذه الأفعال.[5]

ثالثا: الأفعال المكونة لجنحة التعامل في المصنفات المقلدة

---

[1] - حاج صدوق لبندة، المرجع السابق، ص. 25.

[2] - المادة 52 من الأمر رقم 03-05 سالف الذكر.

[3] - المادة 152 من الأمر رقم 03-05 سابق الذكر.

[4] - راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل في العلوم الإنسانية و الاجتماعية، العدد 34، جوان 2013، ص. 143.

[5] - بن حليمة ليلى، المرجع السابق، ص. 125.

لقد وسع المشرع الجزائري من نطاق الحماية للمصنفات الرقمية من جرائم التقليد لتشمل كافة التصرفات الواردة على المصنفات المقلدة سواء كانت ناقلة للملكية أو للاستغلال و الانتفاع فقط، و يكون المصنف مقلداً إذا كان مشابهاً كليةً أو جزئياً للمصنف الأصلي الذي يحميه القانون.[1]

تأسيساً على ذلك، يعد مرتكبا لجنحة التقليد، كل يقوم بالتعامل في النسخ المقلدة بغض النظر عن مكان تقليدها سواء في أرض الوطن أو خارج حدوده، و ذلك على النحو التالي:

1- **استيراد نسخ مقلدة من المصنف الرقمي و تصديرها:** يتمثل هذا التقليد في كل عمليات إدخال المصنفات المقلدة إلى التراب الوطني أي إستيرادها، و كذا إخراجها منه أي تصدريها.

2- **بيع نسخ مقلدة من المصنف الرقمي:** يقصد بذلك القيام ببيع نسخ مقلدة من المصنف الرقمي بعد الحصول عليها في شكلها المقلد أو القيام باستنساخ نسخ مقلدة ثم التصرف فيها عن طريق البيع.

3- **تأجير مصنف رقمي مقلد أو عرضه للتداول:** يشمل هذا النوع من التقليد كل تصرفات التأجير التي ترد على نسخ مقلدة من مصنف رقمي لمدة معينة، و كذلك كل صور التداول في السوق لهذه النسخ المقلدة سواء كان التصرف نقل ملكية أو نقل حق الانتفاع.[2]

و تعتبر جنحة التعامل في المصنفات المقلدة بجميع صورها سالفة الذكر من الجرائم العمدية التي تتطلب لقيامها توفر القصد الجنائي، من خلال علم الجاني بأنه يتعامل في مصنفات مقلدة سواء داخل الوطن أو خارجه إما بالبيع أو التأجير أو الاستيراد أو التصدير أو أية صورة أخرى للتداول، وأن تتجه إرادته إلى القيام بهذه الأفعال المجرمة.[3]

الفرع الثاني: الجزاءات المقررة لجرائم تقليد المصنفات الرقمية

حدد المشرع الجزائري العقوبات المقررة على مرتكب جنحة التقليد على النحو التالي:

---

[1] - محمد علي سكيكر، الجريمة المعلوماتية و كيفية التصدي لها، دار الجمهورية للصحافة، الطبعة الأولى، السلسلة كتاب الجمهورية، مصر، 2010، ص. 149.

[2]- نايت أعمر علي، الملكية الفكرية في إطار التجارة الالكترونية ، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013-2014، ص. 81-82.

[3] - محمد علي سكيكر، المرجع السابق، ص. 150.

أولا: العقوبات الأصلية

تشمل عقوبة سالبة للحرية تمثل في الحبس من ستة أشهر إلى ثلاث سنوات، وغرامة مالية من 500.000 دينار جزائري إلى 1.000.000 دينار جزائري و ذلك سواء تمت عملية النشر داخل الجزائر أو خارجها[1]، على أن تضاعف العقوبة في حالة العود مع جواز تقرير الغلق المؤقت لمدة لا تتعدى 06 أشهر للمؤسسة التي يستغلها المقلد أو شريكه أو تقرير الغلق النهائي عند الاقتضاء.[2]

ثانيا: العقوبات التكميلية[3]

يجوز للجهة القضائية المختصة أن تقرر:

- مصادرة المبالغ المحصلة من جنحة التقليد و مصادرة وإتلاف العتاد المستعمل خصيصا للتقليد و كذا النسخ المقلدة.
- مصادرة المبلغ الذي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي للمصنف محمي.
- مصادرة وإتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة. [4]

كما يجوز للجهة القضائية المختصة أن تأمر بناء على طلب الطرف المدني نشر أحكام الإدانة كاملة أو مجزأة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها ومن ضمن ذلك على باب مسكن المحكوم عليه وكل مؤسسة أو قاعة حفلات يملكها، على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها. [5]

و تأمر الجهة القضائية المختصة في جميع الحالات المنصوص عليها بالمادتين 151 و152 من الأمر 03-05 بتسليم العتاد أو النسخ المقلدة أو قيمة كل ذلك كله وكذلك الإيرادات أو أقساط الإرادات موضوع المصادرة للمؤلف أو لأي مالك حقوق آخر أو ذوي حقوقهما لتكون عند الحاجة بمثابة تعويض عن الضرر اللاحق بهم. [6]

---

[1] - المادة 153 من الأمر رقم 03-05 سالف الذكر.

[2] - المادة 156 من الأمر رقم 03-05 سابق الذكر.

[3] - المواد 156 إلى 159 من الأمر رقم 03-05 سالف الذكر.

[4] - المادة 157 من الأمر رقم 03-05 سالف الذكر.

[5] - المادة 158 من الأمر رقم 03-05 المذكور أعلاه.

[6] - المادة 159 من الأمر رقم 03-05 سابق الذكر.

خاتمة:

لقد حاول المشرع الجزائري بمقتضى المواد من 143 إلى 160 من الأمر 03-05 سابق الذكر توفير الحماية القانونية لحقوق المؤلفين على مصنفاتهم الفكرية سواء من جانبها المادي أو المعنوي، من خلال تكريسه لآليات تكفل الحماية المدنية لأصحاب هذه الحقوق، **كما اعتمد من جانب آخر على آليات جزائية لردع مرتكبي جرائم التقليد الماسة بحقوق المؤلفات الأصلية.**

كل ذلك، يبرز أهمية دراسة مدى تأثر أحكام هذا الأمر بالتطورات التقنية الحديثة التي أفرزتها الثورة المعلوماتية و مدى مواكبته للتطور السريع في مجالي الكمبيوتر و الاتصالات، لاسيما في ظل انتشار جرائم التقليد **الواقعة على** المصنفات الرقمية التي تمثل اعتداء على الحقوق المعترف بها لمؤلفيها، و ذلك بالنظر إلى طبيعة العالم الرقمي و طريقة إتاحته إلى الجمهور، و كذلك صعوبة مراقبة محتوى شبكات الانترنت.[1]

و بناء على ما سبق بيانه، يتضح حرص المشرع الجزائري على حماية حقوق المؤلف في البيئة الرقمية فيما يلي:

- توسيع مجال الحماية لجميع الإبداعات الفكرية مهما كان شكلها أو طريقة التعبير عنها طالما كانت تتميز بالابتكار أو الأصالة و مثبتة بدعامة تظهر وجودها المادي، و بالنظر لما يبذله مبدعو المصنفات الرقمية بشتى أنواعها من مجهودات في سبيل صياغتها وتصميمها وإتاحتها للجمهور عبر الوسائل الالكترونية، فإنها تستحق الحماية القانونية، و ذلك بالرغم من طبيعتها وخصوصيتها لاسيما من حيث تعدد دعائمها الرقمية، و كذا سرعة بثها و نشرها عبر شبكة الانترنت.
- اعتبر المشرع الجزائري صراحة برامج الحاسوب من بين المصنفات الأدبية و الفنية المشمولة بالحماية القانونية، لكنه في المقابل لم يفرق في حماية هذه البرامج بين أنواعها المختلفة.
- قد يظهر من الناحية النظرية أن الأمر 03-05 يتسم بالمرونة عندما فسح المجال واسعاً أمام التطور التكنولوجي لظهور مصنفات رقمية جديدة، إلا أنه و مع الانتشار الواسع لهذه المصنفات و تعقيدات استخدامها والإشكالات المثارة حولها، أثبتت أحكامه من الناحية العملية قصورها في مواجهة بعض حالات التقليد لاسيما بالنسبة لبرامج الحاسوب و قواعد البيانات على الخط و كذا محتوى مواقع الانترنت.

[1]- كوثر مازوني، المرجع السابق ص. 49-50.

- تكمن آليات حماية حقوق المؤلف على مصنفاته الرقمية في وسائل تحفظية وقائية خول القانون بموجبها لرئيس الجهة القضائية صلاحية الأمر باتخاذ إجراءات و تدابير تحفظية مؤقتة استعجالية لغرض الحيلولة دون حدوث تعدي على الحقوق المحمية، وكذا الحفاظ على الأدلة ذات الصلة بالتعدي، وذلك بطلب من مالك الحقوق المتضرر أو ممثله.
- فضلا عن ذلك تمنح الدعوى المدنية للمؤلف الحق في المطالبة بالتعويض عن الضرر المادي و المعنوي الذي لحق بمصنفاته الرقمية أو بسمعته من جراء أفعال التقليد.
- كذلك أقر المشرع الجزائري إمكانية اتخاذ آليات قمعية وردعية تتضمن عقوبات جزائية على كل من ينتهك حقوق المؤلف المنصوص عليها في المواد من 151 إلى 160 من الأمر 03-05 و التي حدد بموجبها الأفعال المجرَمة و العقوبات المقررة لها.
- بناء على تعداد المشرع الجزائري للأفعال المكونة لجنحة التقليد تتنوع صور هذه الجنحة، فمنها ما يشكل إعتداء مباشر على الحقوق الأدبية و المالية للمؤلف، و منها ما يمثل اعتداء غير مباشر عليها كجرائم التعامل في المصنفات المقلدة، و تتسم جل هذه الأفعال بالطابع التقليدي و مع ذلك تبقى هذه الاعتداءات قابلة للممارسة على المصنفات الرقمية.
- يلاحظ على العقوبات المقررة في التشريع الجزائري أنها غير مشددة مقارنة مع العقوبات المنصوص عليها في التشريعات المقارنة، و التي تصل إلى عقوبة السجن كعقوبة سالبة للحرية، أو تكون متباينة بحسب نوع التعدي محل جنحة التقليد وجسامته.
- تعد الغرامة المالية غير كافية لردع مرتكبو جرائم التقليد مقارنة مع رقم الأعمال الذي سيحققونه من جراء عمليات التقليد، لذا فمن باب أولى ترك تقديريها للسلطة التقديرية للقاضي مع إمكانية تحديد حد الأدنى لها، بما يتناسب و القيمة الاقتصادية المتوقع تحقيقها من وراء حماية هذه المصنفات التي تمثل مظهر من مظاهر التقدم العلمي والتكنولوجي.

و بالرغم من هذه الخطوات التي اتخذها المشرع الجزائري في مجال مكافحة جرائم التقليد الواقعة على حقوق المؤلف، إلا أنها لا تماشي و إبداعات المؤلفين المتأثرة بالتطور الحاصل في مجال تقنية المعلومات و شبكة الاتصالات، و هذا ما يدفعنا إلى اقتراح التوصيات التالية:

- تعديل نصوص الأمر 03-05 المتعلقة بجرائم التقليد و التي أظهرت قصور واضح في التصدي لهذه الجرائم المستحدثة، و ذلك من خلال تبني أحكام قانونية ملائمة لطبيعة

هذه المصنفات المتاحة عبر شبكة الانترنت خاصة منها برامج الحاسوب المتطورة في هذا المجال.

- استحداث إجراءات قضائية سريعة و فعالة في مكافحة جرائم التقليد بما يتناسب مع طبيعتها الرقمية و مع تنوع صورها، خاصة بعدما أثبتت أحكام الحجز التحفظي قصور في تطبيقها على بعض المصنفات الرقمية أمام الوسائل التكنولوجية الحديثة المستخدمة في تقليدها، و من أبرز صور هذا القصور تعذر إمكانية الحجز على شبكات الحاسوب و على محتوى مواقع الانترنت.
- تطوير الأجهزة المعنية بمكافحة جرائم التقليد الواقعة على حقوق الملكية الرقمية من خلال دعمها بالإمكانيات المادية و التقنية التي تمكنهم من أداء مهامهم بفاعلية، مع رفع كفاءة العنصر البشري فيها و ذلك بتدعيم خبراتهم العلمية و الفنية في مجال المعلوماتية.
- تشديد العقوبات على جرائم التقليد نظرا لجسامة الأضرار و الخسائر الناجمة عنها، ذلك أن سهولة أعمال التقليد في بيئة الإنترنت يؤدي إلى ضياع الحق المالي والأدبي للمؤلف، مما قد يتسبب في إحجامه عن الإبداع الفكري.
- ضرورة تبني أساليب الحماية التقنية الالكترونية للمعلومات المخزنة على الدعامات الرقمية و المنشورة في شبكة الانترنت، كالتشفير و كلمات المرور و غيرها من التقنيات الحديثة بهدف الحد من جرائم الاعتداء على حقوق الملكية الرقمية.

إشكالية تطبيق النصوص التقليدية على سرقة المال المعلوماتي للبنوك

The problem of applying traditional texts to stealing information money for banks

د.بوزيدي الياس أستاذ محاضر " أ "

معهد الحقوق والعلوم السياسية

المركز الجامعي مغنية - الجزائر

مقدمة

تشير الجرائم الإلكترونية عمومًا إلى جميع الجرائم المتعلقة باستخدام التقنيات الجديدة وبشكل أكثر تحديداً ، يتعلق الأمر "بجميع الجرائم الإجرامية المحددة المتعلقة بتكنولوجيا المعلومات والاتصالات ، وكذلك الجرائم التي يُسهل ارتكابها أو يرتبط باستخدام هذه التكنولوجيات.

وبعبارة أخرى ، يتعلق الأمر بالجرائم الجنائية المرتكبة عبر شبكات الكمبيوتر ، على وجه الخصوص ، على الإنترنت. ويغطي فئتين رئيسيتين من الجرائم: الجرائم المرتبطة مباشرة بتكنولوجيا المعلومات والاتصالات (الأشكال المختلفة للقرصنة الحاسوبية ، والهجمات على أمن وسائل الدفع على الإنترنت ، وما إلى ذلك) وتلك التي عند ارتكابها تقوم بتسهيل أو ربط استخدام هذه التقنيات (نشر محتوى غير قانوني ، والجرائم ضد الممتلكات ، والتزوير ، والضرر على الأشخاص[1].

يشير مفهوم "الجريمة السيبرانية" ، الذي يتم استخدامه بشكل متكرر أكثر على الرغم من أنه في بعض الأحيان غير محدد بدقة ، يشير من حيث المبدأ إلى توصيف إجرامي ، ولكنه ليس محدداً أو موحدًا في النظم القانونية المختلفة. في الاستخدام الحالي ، وهو المستخدم هنا ، يتم استخدامه لتعيين جميع أشكال الهجمات التي تتم عن طريق شبكات الكمبيوتر أو أنظمة المعلومات ، أو استهدافها[2].

[1] Chilstein David. Législation sur la cybercriminalité en France. In: Revue internationale de droit comparé. Vol. 62 N°2,2010. P.553.

[2] Édouard fernandez-bollo، institutions financières et cybercriminalité، revue d'économie financière، 2015/4 (n° 120)، p.181.

تأليف مجموعة من الباحثين

إن تأثير التطورات التكنولوجية المستحدثة على أساليب التعامل في مختلف المجالات، كان له الأثر البالغ على البيئة التجارية عموما و على النشاط المالي و المصرفي بوجه خاص.

إن المصارف و البنوك تمارس عديدا من الأنشطة التجارية، باعتبار أن العمليات المصرفية عمل تجاري بحسب موضوعه ، و الملاحظ أن هذه الأخيرة(العمليات المصرفية) ،قد وصلت إلى درجة عالية من الكفاءة التقنية بحيث أصبحت تواكب تطورات الثورة المعلوماتية في زمن العولمة.

إن استخدام الحاسب الآلي وشبكات المعلومات قد أصبحت من الوسائل التي يشوبها كثير من المخاطر، مما ينطوي على ذلك ضرر بالنسبة للذمة المالية للبنوك، حيث أن الاستخدام غير القانوني للتكنولوجيا يؤدي إلى السرقة والاحتيال والتلاعب في البيانات المالية، وهذا من شأنه انتهاك الثقة والصلاحية في العمليات المالية المتبادلة عن طريق الوسائل الالكترونية.

إن مسألة سرقة المال المعلوماتي لقد أثار الكثير من الجدل، لقد تم الاعتراف منذ فترة طويلة بأن محله لا يمكن أن يكون غير مادي، وتكمن الإشكالية الأساسية في مدى تطبيق نصوص العقوبات التقليدي على جريمة سرقة المال المعلوماتي لدى البنوك ، على اعتبار أن هذه النصوص وضعت أساسا لحماية الأشياء المادية في مواجهة صور التعدي المألوفة، والذي يتعذر معه تقرير المسؤولية الجزائية على أفعال التعدي لمكونات الأنظمة المعلوماتية ذات الطابع المعنوي بالسرقة، ومن جهة أخرى أن تطبيق هذه النصوص قد يتعارض أحيانا والطابع الخاص للوسائل المعلوماتية المستحدثة لتنفيذ الجريمة.

ولهذا سنتعرض إلى الطبيعة القانونية للمال المعلوماتي محل السرقة (مطلب أول) إشكالية تقرير المسؤولية الجزائية لسارق المال المعلوماتي لدى البنوك (مطلب ثان).

المطلب الأول: الطبيعة القانونية للمال المعلوماتي محل السرقة

تتجلى إشكالية البحث هنا، على اعتبار أن المعلومات الالكترونية والبرامج الحاسوبية هي نوع جديد من الأموال ذات القيمة الاقتصادية الكبيرة، والتي تستعص بسبب طبيعتها غير المادية على تشمليها بنصوص جرائم الأموال الموجودة.

ولهذا سنتعرض إلى مدى انطباق وصف المال على المعلومات (الفرع الأول)، والى مدى اعتبار المعلومة محلا لجريمة سرقة المال المعلوماتي (الفرع الثاني)

الفرع الأول: مدى انطباق وصف المال على المعلومات

استقر الفكر التقليدي على مفهوم ثابت للمال تم اعتماده طبقا لما ورد من نصوص تجرم الاعتداء عليه في قانون العقوبات، بحيث يشترط فيه إن يكون مالا ماديا وان تكون له قيمة وان يكون مملوكا للغير.

ويراد بالمال في عرف جريمة السرقة، كل شيء يصلح محلا لحق عيني، وعلى وجه التحديد حق الملكية. والشرط الأساسي لصلاحية الشيء محلا لحق عيني هو كونه نافعا للإنسان، ونفعه والتنافس على الاستئثار به يعني وجوب كونه ذا قيمة، أو في تعبير آخر" متقوما "[1].

والمال المنقول يشترط أن يكون ماديا، فإذا كان المال شيء غير مادي(شيء معنوي) وليس له كيان ملموس، فلا يمكن تصور اختلاسه[2]. وهكذا فلو نسب شخص لنفسه نظرية جديدة في علم الرياضيات في حين يكون اطلع عليها من آخر، الى غير ذلك من الوقائع، لا يكون سارقا، لأن الحقوق المشار إليها حقوق معنوية غير مادية، ولا تصلح محلا للاختلاس، وهذا بطبيعة الحال مالم يصبح للحق المعنوي كيان مادي، حيث يصبح اختلاسه إذ ذاك سرقة، ونحو ذلك أن يدون عالم الرياضيات نظريته الجديدة في أوراق ويقوم آخر بالاستيلاء عليها وينسبها لنفسه، أو يقوم مخترع بتدوين اختراعه في وثيقة ويقوم آخر باختلاسها[3].

ويجب أن يكون المال أو الشيء منقولا، لاستحالة سرقة العقارات لعدم نقلها كما هي من مكانها. ويعتبر منقولا كل شيء في الإمكان نقله من جهة لأخرى. وهذا طبقا للمعنى في القانون الجنائي لأنه يختلف عن معنى المنقول الذي نص عليه القانون المدني واعتبره عقارا بالتخصيص، ومثاله نوافذ المنزل، وسرقة شجرة من حديقة بعد قطعها[4].

---

[1] محمود نجيب حسني، جرائم الاعتداء على الأموال، منشورات الحلبي الحقوقية، ط.3، بيروت، لبنان، 1998، ص ص.35-36.

[2] M.-L. RASSAT, Droit pénal spécial. Infractions du Code pénal, 7 e éd., 2014, Précis Dalloz, § 104 s.

[3] عبد الواحد العلمي، شرح القانون الجنائي المغربي، القسم الخاص، مطبعة النجاح الجديدة، الدار البيضاء، المغرب،2013، ص.344.

[4] محمد صبحي نجم، شرح قانون العقوبات الجزائري، القسم الخاص، ديوان المطبوعات الجامعية، الجزائر، 2000،ص.122.

كما يلزم أن يكون المال المنقول غير مملوك للجاني، ومن ثم يكفي لقيام جريمة السرقة أن يكون الشيء المسروق غير مملوك للجاني، ومن ثم فمن يختلس منقولا كان قد آل إليه بالميراث أو الهبة أو الوصية، وهو لم يكن يعلم بذلك لا يعتبر سارقا لذلك المنقول[1].

وعلة هذا الشرط أن السرقة اعتداء على الملكية، ولا يتصور هذا الاعتداء إلا إذا نال الفعل مالا يتعلق به حق ملكية الغير، ذلك انه إذا انصب على مال يملكه مرتكب الفعل فهو استعمال لحقه على الشيء[2].

وبخصوص طبيعة المال في المعلوماتية، فهناك المال المعلوماتي المنطقي والمال المعلوماتي الطبيعي (الأجهزة)، فيعرف هذا الأخير على انه المكونات المادية لعناصر النظام المعلوماتي التي تحتوي على المعلومات ولها كيان مادي ظاهر وملموس والمتمثلة بوحدات العرض والتسجيل والشاشة وملحقات الجهاز والحاسب الآلي من أجهزة إدخال وإخراج (الطابعات، السماعات وغيرها) وكذلك الشرائط الممغنطة والدسكات[3].

والمال المعلوماتي الطبيعي يصلح لأن يكون محلا للسرقة باعتباره مال مادي ملموس ويمكن نقله وحيازته والاستيلاء عليه، ومن ثم فالمعلومات المخزنة عليه تصلح لان تكون محلا للسرقة[4].

والمال المعلوماتي المنطقي، والذي يطلق عليه بالمكونات Software ويسميها البعض بالبرمجيات، ويسميها آخرون بالكيان المنطقي، ويحصرها فريق ثالث بالمعلومات، ورابع بالمعطيات. وعلى أية حال أن أصح التسميات هي (العناصر أو المكونات غير المادية للحاسب)، لأن تعبير الكيان المنطقي غامض ومن شانه أن يقود الى دلالات أخرى لا علاقة لها بالمعلوماتية، كما أن

---

[1] إسحاق إبراهيم منصور، شرح قانون العقوبات الجزائري، جنائي خاص، في الجرائم ضد الأشخاص والأخلاق وامن الدولة، ديوان المطبوعات الجامعية، الجزائر، 1988. ص.142.

[2] محمود نجيب حسني، المرجع السابق، ص. 50.

[3] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2017-2018، ص.183.

[4] هدى قشقوش، جرائم الاعتداء على الحاسب الآلي في القانون المقارن، دار النهضة العربية، 1990، ص.56.

تعبيرات برامج أو برمجيات ومعلومات ومعطيات هي تعبيرات قاصرة عن استيعاب مضمون هذه العناصر[1]. أو هو المعلومات المختزنة داخل النظام المعلوماتي وليست المتنقلة من خلاله[2].

لقد اختلف في طبيعة المعلومة الرقمية في مدى اعتبارها مالا أو شيئا يقوم بالمال، ففي بادئ الأمر كان الاعتراف بصفة المال مقصورا على الأشياء المادية الملموسة، التي تكون محلا للتملك، الأمر الذي تغير بعد ذلك فأصبح وصف المال يستشف من القيمة الاقتصادية للشيء، مما يعطي صفة المال للمعلومة ذات القيمة الاقتصادية.

ويستدل في ذلك أنه فيما يتعلق تجريم الطاقة رغم طبيعتها، بحيث جرم الاعتداء عليها باعتبارها مالا ذا كيان مادي لا شيئا ماديا، لها قيمة، يتحقق الاستيلاء عليها بالاستيلاء على قيمتها ومنفعتها، فالكهرباء عدت من قبيل الأشياء المادية لكونها تمر داخل كابلات يمكن ملاحظتها، كذلك الحال، بالنسبة للمعلومات فهي تسير أيضا عبر أسلاك يمكن ملاحظتها، كما أنه حتى عند مرورها من خلال تيار غير مطرد (الانتقال الكهرومغناطيسي) فانه من الممكن قياسها من خلال وحدة القياس المعلوماتي، ويمكن رؤيتها من خلال شاشة الحاسب الآلي.

كما أن المعلومات إذا ما تمت معالجتها آليا تصبح بيانات أو معطيات ذات كيان مادي يتمثل في نبضات الكترونية أو إشارات الكترونية ممغنطة يمكن تخزينها على وسائط معينة ونقلها وبثها وجحيتها واستغلالها وإعادة إنتاجها، فضلا عن إمكانية قياسها، ومن ثم فهي ليست شيئا معنويا[3].

إن التطور الحاصل في مجال تكنولوجيا المعلومات، أدى الى إعطاء الأموال المعنوية قيمة اقتصادية قد تفوق قيمة الأموال المادية، الأمر الذي أدى الى البحث عن معيار جديد غير معيار مادية المال أو طبيعة الشيء الذي يرد عليه الحق المالي، نصل من خلاله الى إصباغ صفة المال على الشيء المعنوي. وان معيار القيمة الاقتصادية للشيء يعتبر الشيء مالا، لا بالنظر الى ماله من كيان مادي وإنما بالنظر الى قيمته الاقتصادية[4].

---

[1] وسيم طعمة، السرقة المعلوماتية، دراسة مقارنة، مجلة جامعة البعث، المجلد 39، العدد 68، 2017، ص.158.

[2] رابحي عزيزة، المرجع السابق، ص. 184.

[3] كوثر شريط، سرقة المعطيات المعلوماتية، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، المجلد8،العدد 2، جوان 2017، ص. 392.

[4] كوثر شريط، المرجع نفسه، ص.392.

ولكي تتمتع المعلومات بالحماية الجنائية لابد من توافر شروط تتمثل في[1]:

أولا: التحديد والابتكار فالتحديد أي أن المعلومة قبل كل شيء تعبير وصياغة مخصصة من أجل ذلك، وتبلغ أو يمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة الى الغير. ويتمثل الابتكار في أن المعلومة لا تكون شائعة ومتاحة للجميع ولا يمكن الوصول إليها أو نسبتها الى شخص محدد.

ثانيا: السرية والاستئثار فالمعلومة السرية هي التي لا يمكن الوصول إليها بسهولة واستخدامها يكون قليل وبالتالي يكون حصرها في دائرة السرية. أما توافر صفة الاستئثار للمعلومة إذا كان الوصول إليها غير مصرح ب هالا لأشخاص محددين ويمكن أن ينبع الاستئثار من سلطة شخص أو جهة ما على المعلومة أو على التصرف فيها.

وهناك من يشترط أن تكون المعطيات معالجة أليا لكي تخضع للتجريم، أضف الى ذلك انه لابد من اتخاذ صاحبها إجراءات وتدابير جدية لحمايتها والمحافظة على سريتها.

وبناء على ما للمعلوماتية من قيم اقتصادية ومالية، إذ أن المعلومات تعتبر مالا منقولا وتتمتع بحق الحماية، يستوي في ذلك أن تكون المعلومة مبتكرة، فهي محمية بتشريعات حماية حقوق المؤلف وأحكام الملكية الفكرية.[2]

بل أكثر من ذلك، يرى بعض الفقه[3] أن الأحكام القانونية المتعلقة بحماية حقوق المؤلف مستمدة حرفيا من التشريع الفرنسي، ولذا ليس من المستبعد أنها ستتغير في المستقبل لإخضاع برامج الحاسوب لنظام " براءة الوسيلة".

وهذا كله يدل على القيمة الاقتصادية والمالية، وكذا التطور الهائل لتكنولوجيا المعلومات وحماية الثورة المعلوماتية من الاعتداء.

الفرع الثاني: مدى اعتبار المعلومة محلا لجريمة سرقة المال المعلوماتي

---

[1] رابحي عزيزة، المرجع السابق، ص ص.31-34.

[2] المادة 4(أ) من الأمر 2003-05 المؤرخ في 19 يوليو 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة، ج ر، العدد 44، المؤرخة في23 يوليو 2003.

[3] فرحة زراوي صالح، الكامل في القانون التجاري، الحقوق الفكرية، ابن خلدون للنشر والتوزيع، وهران، الجزائر، 2006، ص.35.

إن أبرز إشكال يطرح بخصوص سرقة المعلومات الرقمية، يكمن في مدى قابليتها للاختلاس، الأمر الذي انقسم فيه الفقه إلى رأيين، وفق ما يلي:

أولا: ويرى أصحاب الرأي الأول أن المعلوماتية ليست مالا ويخضع للسرقة، وذلك على اعتبار أن جريمة السرقة هو اعتداء على حق عيني هو حق الملكية، ومن أساسيات الحق العيني أن يكون له كيان مادي محسوس يستطيع صاحبه أن يمارس عليه سلطاته[1]. وأن الأموال غير المادية هي الاموال الغير مجسدة ومن ثم فان المعلومة وحده لا تصلح أن تكون محلا للسرقة مادامت منفصلة عن سندها المادي " قرص ممغنط، ورقة..."[2].

بل أكثر من ذلك، فان جريمة السرقة تتطلب نقل الحيازة المادية من مالكه أو حائزه الى الجاني، وهو ما لا يتوافر لدينا في حالة سرقة المعلومات أو البيانات، فتظل هذه الأخيرة في حيازة صاحبها، كما قد تنسخ ولا تنقل[3].

وباعتبار أن المعلوماتية ليست مالا، فان المقومات المعنوية من النظام المعلوماتي يمكن ان تستغل ماليا، فالقابلية للاستغلال المالي لا تعني أنها واردة على شيئ يعتبر مالا في ذاته، ومن هنا لا يمكن وقوعها محلا لجريمة السرقة.

كما أن المعلومات قد تكون سرية والاطلاع عليها أو حيازته محظور، وبالتالي فان الحصول عليه ممن ليس لديه الحق يمثل انتهاكا لسرية المعلومات وليست سرقة لها، بل أكثر من ذلك فان المعلوماتية لا تصلح أن تكون مالا أو محلا للسرقة إلا إذا اقترنت بالمادية لذلك فان التعدي عليها بالسرقة لا يعتد به[4].

---

[1] وسيم طعمة، المرجع السابق، ص.160.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجرائم ضد الاشخاص والجرائم ضد الاموال، الجزء الاول، الطبعة الثالثة، دار هومة، الجزائر، 2006، ص.259.

[3] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص. 97.

[4] رابحي عزيزة، المرجع السابق، ص.184.

كما أن المال المعلوماتي قبل أن يكون مجرد قيمة هو إبداع فكري، جاء بنتيجة جهد وفكر صاحبه، ولا يصلح بالتالي لأن يكون محلا لجريمة السرقة وما في حكمها في هذا الشأن، بل لجرائم المساس بالملكية الفكرية[1].

ثانيا: أما عن أصحاب الرأي الثاني أن المعلوماتية تعتبر مالا ويخضع للسرقة، وذلك على اعتبار أن لها قيمة مالية ويمكن من خلالها أن تخضع للسرقة، حيث أن المعلومات من الأفكار تحتوي على رسالة يمكن إدراكها عند الحفظ أو النقل أو المعالجة.

فالمعلومات ناتج تكوين نسق فكري لمبتكرها أو مبتدعها ويترتب عليها وجود علاقة بين المعلومات ومبتكرها، فيكون له نقلها وإيداعها وحفظها وتأجيرها وبيعها، فالمعلوماتية تعتبر أموالا ذات قيمة اقتصادية حيث أنها تطرح في الأسواق للتداول مثل اي سلعة ولها سوق تجاري يخضع لقوانين السوق الاقتصادي[2].

كما أن البيانات التي تمت معالجتها الكترونيا فتتحدد في كيان مادي يتمثل في نبضات أو إشارات الكترونية ممغنطة يمكن تخزينها على وسائط معينة ونقلها، فضلا عن إمكانية حجبها واستغلالها وإعادة إنتاجها وتقديرها كميا، فهي ليست شيئا معنويا كالأفكار بل شيئا له في العالم الخارجي وجود مادي ولكنه غير محسوس.

فضلا على إمكانية اعتبار البرنامج مالا حكميا، من منطلق إمكانية وقوع فعل الاختلاس على الكهرباء، حيث أنها تدخل في عداد الأشياء المادية التي تقبل التملك والحيازة، ولذلك يقرر صلاحية البرمجيات لتكون محلا لجرائم المال على أساس اعتبارها من قبيل الأموال المادية المحرزة، فيعتبرون أن سرقة برامج وأسرار الحاسب هي سرقة مادية متوافرة الأركان والشروط[3].

كما انه وانطلاقا من تعريف السرقة وفقا للقانون الفرنسي تمتد لتشمل الأشياء المعنوية ومنها المعلومات، إذ أن المال بمفهومه التقليدي الذي يتمثل بالصفة المادية المنقولة، كان يرتبط بالوقت الذي ظهرت فيه جريمة السرقة، وما كان متواجدا في تلك الفترة من أنواع للمال تغلب عليها

---

1 وسيم طعمة، المرجع السابق، ص.161.

2 رابحي عزيزة، المرجع السابق، ص.185.

3 وسيم طعمة، المرجع السابق، ص ص.163-164.

الصفة المادية، ولولا ذلك لكانت جريمة السرقة شاملة لأنواع أخرى من المال، وبناء غليه ينبغي مع ظهور القيم المعلوماتية أن تكون هذه القيم مشمولة بأحكام السرقة وإساءة الائتمان[1].

المطلب الثاني: إشكالية تقرير المسؤولية الجزائية لسارق المال المعلوماتي لدى البنوك

يتمثل موضوع السرقة في الشيء ويقع عليه الاعتداء، ونتعلق به الحقوق والمصالح التي يحميها القانون ويتعين أن يكون هذا الشيء ذو طبيعة مادية، علاوة على كونه مملوكا للغير.

وهذا ما يثير إشكالات قانونية عند تطبيقها على المال المعلوماتي، وهذا ما سنعالجه من خلال التعرض أركان جريمة سرقة المال المعلوماتي (فرع أول) والى موقف التشريع الجزائري والفرنسي من جريمة سرقة المال المعلوماتي (فرع ثان) ، ومظاهر سرقة المال المعلوماتي لدى البنوك (فرع ثالث).

الفرع الأول: أركان جريمة سرقة المال المعلوماتي

انطلاقا من نص المادة 350 من قانون العقوبات الجزائري، التي تقضي بأنه كل من اختلس شيئا غير مملوك له يعد سارقا، ويعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 100.000 دج إلى 500.000 دج.

وهكذا يتبين لنا أن هذه الجريمة تقوم على توافر ركنيين أولهما الركن المادي (فعل الاختلاس)، وثانيهما القصد الجنائي.

أولا: الركن المادي (فعل الاختلاس)

يتحقق الاختلاس بفعل مادي يتم بانتزاع الشيئ من مالكه أو حائزه، ونقله الى حيازة الجاني الشخصية أي حيثما أراد للشيئ أن يكون، بحيث يصبح تحت تصرفه شخصيا، ولا يشترط أن الجاني هو الذي يقوم بأخذ الشيئ أو نقله بل يكفي أو يهيئ الوسيلة لنزعه من حيازة المجنى عليه. ولقد تطور تعريف الاختلاس بأنه الاستيلاء على حيازة الشيئ بعنصريها المادي والمعنوي معا، بدون علم وعلى غير رضا مالكه أو حائزه السابق. ويقصد بذلك إلى عدم اشتراط أن يكون الجاني بفعله المادي انتزع حيازة الشيئ، بل يكفي أن يسلب الجاني حيازة الشيئ بدون علم وبدون رضا المالك أو الحائز السابق لذلك الشيئ[2].

---

[1] رابحي عزيزة، المرجع السابق، ص.185؛ وسيم طعمة، المرجع السابق، ص ص.163.

[2] اسحاق ابراهيم منصور، المرجع السابق، ص ص.142-143.

إن سرقة المعلوماتية المخزنة في النظام المعلوماتي تتعدد صورها، وكذلك في مدى صلاحيتها لاعتبارها ركنا موكنا للسرقة.

أ - **النسخ غير المشروع للمعلومات:** ان الشخص الذي يحصل على معلومات مختزنة في جهاز حاسوب شخص آخر بحيث لا يؤدي الى حرمان الشخص صاحب المعلومات من المعلومات المختزنة في جهازه اذ لم يؤخذ منه شيئ، وكل ما في الأمر أن المعتدي قام بنسخ هذه المعلومات أو تصويرها ويكون ذلك قد تقاسم الاطلاع على هذه المعلومات مع صاحبه، بالاضافة انه لم تقم لديه نية حرمان صاحب المعلومات مما أخذه مؤقتا أو دائما، والمشكلة هل هذه الواقعة تعد من قبيل السرقة ؟

ولقد اختلف من حيث صلاحية نسخ ونقل المعلومات من النظام المعلوماتي للاختلاس الى رأيين[1]، حيث يرى الرأي الأول منهما عدم صلاحية نسخ ونقل المعلوماتية في النظام المعلوماتي حتى لو أدى ذلك في بعض الأحيان إلى الإضرار بها وإتلافها أو التأثير على قيمتها، وذلك على اعتبار:

- عدم تصور انتزاع حيازة هذه المعلومات ولا تكون محلا للسرقة إلا إذا وقعت داخل إطار مادي.
- أن الجاني لم يستولي على أصل المعلومة، ولكنه نقل صورة منها وبالتالي لا ينطبق عليه السرقة، ويعد هذا الفعل تقليدا او سرقة منفعة.

بينما يرى الرأي الثاني صلاحية اختلاس نسخ ونقل المعلومات في النظام المعلوماتي، وذلك على اعتبار:

- يقع فعل الاختلاس على المعلوماتية لوجودها بكل فوائدها الاقتصادية تحت فعل الجاني بمقدوره التصرف فيها بحرية، مع ضرورة وجود نشاط مادي بعد هذا الاختلاس، ويتمثل في بيع المعلوماتية او وضعها موضوع التنفيذ.
- فكرة الاستيلاء الاحتيالي لنسخ ونقل المعلوماتية، هي احدى صور التفسير الواسع للاختلاس.

[1] رابحي عزيزة، المرجع السابق، ص ص.192-193 .

ب - **المعلومات المخزنة على دعامات** وهنا اختلف الفقهاء حول صلاحية المعلومات المخزنة على دعامات للاختلاس الى رأيين[1]، فيرى الرأي الأول عدم الصلاحية للاختلاس بل أنه ينطبق على سرقة الدعامة ذاتها التي توجد عليها المعلومات، وذلك على اعتبار:

- يترتب على سرقة المعلومات والبرامج الموجودة على الدعامة المادية أضرارا تزيد عن قيمتها الحقيقية للدعامة المادية.
- إن اخذ الشيء غير المادي مثل المعلومات لا يكون ماديا إلا إذا كان قد تجسد في هيئة مادية.

أما أنصار الرأي الثاني يرى صلاحية هذه المعلومات للاختلاس وذلك على اعتبار:

- إن سرقة المعلومات وليست الدعامة، هي السبب الذي أدانت من اجله محكمة النقض الفرنسية في قضية " logbax "[2] العامل الذي قام بنسخ المستندات السرية بدون علم ورضا المالك.
- إن محكمة النقض الفرنسية أدانت شخص، عن جريمة إخفاء لأنه قدم للمحكمة صورة منسوخة كان قد أعدها بنفسه من مستند مسروق بمعرفة شخص مجهول الهوية، فالاختلاس هنا انصب على المعلومات بحد ذاتها.

ومع العلم أن الرأي القائل بصلاحية المعلوماتية المخزنة على دعامات للاختلاس هو الرأي الأكثر تأييدا من جهة الأغلبية.

ثانيا: الركن المعنوي

جريمة السرقة من الجرائم العمدية وهي لا ترتكب دون توافر القصد الإجرامي لدى فاعلها والذي يتكون من العلم والإرادة، أي علم الجاني بأنه يختلس مال غيره دون رضاه ويستولي عليه

---

[1] رابحي عزيزة، المرجع السابق، ص.195.

[2] Crim. 8 janv. 1979, D. 1979. 509, note P. Corlay ; D. 1979. IR 182, obs. G. Roujou de Boubée. – M.-L. RASSAT, in Le rapport de la Cour de cassation [année judiciaire 1979], JCP 1981. I. 3041, no 25.

بنقل حيازته التامة إليه دون سبب مشروع، وأن من شان ذلك أن يجرد المالك من ملكه، وبأن يستولي عليه من شيء له قيمة معتبرة عند مالكه أو حائزه الشرعي ولم يتخلى عنه[1].

إن القصد العام يقوم على العلم الذي ينصب على الجريمة بإرادة تحقيق النتيجة الإجرامية، ولذلك يجب أن يعرف المتهم بان المال مملوك له أو مباح انتفى لديه العلم، وانتفى بالتالي لديه القصد الجنائي. كما انه يجب أن يكون قد تم اخذ المال بدون رضا المجنى عليه، ويختلف رضا المجنى عليه عن علمه، فقد يعلم صاحب المال باستيلاء الغير على ماله ويتركه من اجل استدراكه وضبطه متسلقا بالسرقة، فهنا لا ينتفي القصد الجنائي لدى المتهم، لان العبرة تكون بالرضا الحقيقي.

كما انه يجب أن تتجه إرادة المتهم إلى ارتكاب السرقة واتجاه إرادته إلى تحقيق النتيجة الإجرامية لهذا الفعل، وهي إخراج المال من حيازة المجنى عليه وإدخالها في حيازة شخص آخر، وبهذا يقوم القصد العام في السرقة[2].

إن المجرم المعلوماتي مرتكب لجريمة سرقة المعلومات، يسعى بإرادته الى الاستحواذ عليها بتشغيله للجهاز ويعلم أنها مملوكة لغيره وفي قيامه باختلاسها او نسخها يعتبر قد توافر لديه عنصر القصد العام. كما أن استخدام العميل للسحب من جهاز التوزيع الآلي للنقود لن يتم التغلب عليه إلا إذا تم الربط بين هذه الأجهزة بصرف الأوراق النقدية إلى العميل إلا في حدود الرصيد الذي يوجد في حسابه وقت السحب، وهو ما جرى عليه العمل في نظام السحب من أجهزة التوزيع الآلي للنقود[3].

كما أنه يتطلب الركن المعنوي في السرقة توافر قصد خاص يتمثل في نية تملك المال من طرف المتهم، وتنتفي إرادة المتهم إلى اعتبار المال الذي استولى عليه مملوكا له. كما يجب لتوافر القصد الجنائي توافر نية التملك لحظة ارتكاب السرقة ولا يهم الدافع لارتكاب جريمة السرقة، فالباعث ليس من عناصر القصد الجنائي للسرقة[4].

---

[1] باسم شهاب، جرائم المال والثقة العامة، بيرتي للنشر، الجزائر، 2013، ص.22.
[2] فريجة حسين، المرجع السابق، ص ص.201-202.
[3] رابحي عزيزة، المرجع السابق، ص.197.
[4] فريجة حسين، المرجع السابق، ص.203

فجريمة السرقة المعلوماتية جريمة حديثة تبدأ من أول الدخول غير المشروع الى النظام المعلوماتي، والقصد فيها يتخذ صورتين الأولى تتمثل في حالة الدخول العام، وهو الذي يدخل فيه المستخدم للجهاز والحصول على المعلومات وهو لا يمثل سرقة، أما الثانية والتي تتمثل في انتهاك للنظام المعلوماتي الخاص، والذي له كلمة سر ونظام امني خاص يدل على وجود قصد وسوء نية من مرتكب الفعل. ويتوفر فيها القصد العام والخاص ويظهر القصد الخاص في فترة البقاء غير المشروع إلا أن المشكلة التي تعترض ذلك هي كيفية إثبات سوء النية.

الفرع الثاني: موقف التشريع الجزائري والفرنسي من جريمة سرقة المال المعلوماتي

وفي هذا الصدد، سنتعرض إلى موقف المشرع الفرنسي (أولا)، والمشرع الجزائري (ثانيا) من جريمة سرقة المال المعلوماتي.

أولا: موقف المشرع الفرنسي من جريمة سرقة المال المعلوماتي

على اعتبار أن التكنولوجيا تجعل أسرار حماية البيانات المعلوماتية أكثر هشاشة، ومن ثم قد تتعرض أي شركة أو بنك أو إدارة عامة لدخول النظام المعلوماتي واختلاس البيانات. ومع ذلك تظل هذه البيانات ملكية حصرية للكيان الذي يمتلكها، ولهذا يعد الدخول إلى النظام المعلوماتي لهذه المؤسسة جريمة جنائية.

إن الهدف من هذا الدخول هو اختلاس البيانات المعلوماتية الذي يتكون منها نظام المعالجة الآلية للمعطيات، ومن ثم فان المخاطر ليست محايدة، مما يعني انتهاك البيانات السرية أو أسرار العمل أو حقوق الملكية الفكرية.

يتطور موقف القانون الجنائي بشان الدخول عن طريق الغش لنظام المعلوماتية وسرقة المعطيات التي يتكون منها، ويتضح ذلك من خلال الحكم الصادر في قضية " Bluetouff" التي أصدرتها الغرفة الجنائية لمحكمة النقض الفرنسية في 20 مايو 2015[1]، وهنا محكمة النقض تؤكد

---

[1] « Constitue le délit de maintien frauduleux dans un système de traitement automatisé de données le fait de se maintenir dans ce système après s'y être introduit à la suite d'une défaillance technique et avoir constaté l'existence d'un contrôle d'accès. Le téléchargement, effectué sans le consentement de leur propriétaire, de données que le prévenu savait protégées caractérise la soustraction frauduleuse constitutive du vol. ».

إدانة المدون " Bluetouff " رئيس الصيانة بالاحتيال على نظام المعالجة الآلية للمعطيات والسرقة.

وتتلخص وقائع هذه القضية في قيام "olivier laurelli" المعروف باسم "Bluetouff" وعلى اثر عطل فني في نظام الشبكة الخارجية الخاص بالوكالة الوطنية للأمن الصحي والغذائي والبيئة والعمل ANSES، تمكن مستخدم متصفح بحث " moteur de recherche" من الدخول إلى هذا النظام المحمي عادة باسم مستخدم وكلمة عبور، وقام بتحميل معطيات محمية على عدة دعائم وبثها إلى الغير.

فاتهم بالدخول والبقاء غير المصرح بهما في نظام معالجة آلية للمعطيات وسرقة المعطيات، فبرأته محكمة الدرجة الأولى، لكن على اثر استئناف هذا الحكم من قبل النيابة العامة، أدين من قبل محكمة الاستئناف بباريس[1] بجرمي البقاء غير المصرح به وسرقة المعطيات، وهو القرار الذي طعن فيه بالنقض، لترفض محكمة النقض الفرنسية طعنه على أساس انه ثبت بان " Bluetouff" بقي في نظام المعالجة الآلية للمعطيات بعد اكتشافه بان هذا الأخير محمي، واختلس معطيات استعملها دون رضا مالكها.

والسؤال الذي يطرح هنا: هل يمكن تطبيق أحكام جريمة السرقة وتكييفها مع اختلاس المعطيات المعلوماتية؟

يوضح الحكم المهم الصادر في 20 مايو 2015[2] التغيير في المنظومة، حيث رأت المحكمة إن اختلاس البيانات المعلوماتية دون علم مالكها والمثبتة على دعامة معطيات يشكل سرقة، بالمعنى

Cour de cassation, criminelle, Chambre criminelle, 20 mai 2015, 14-81.336, Publié au bulletin criminel 2015, n° 119.

[1] Cour d'appel de paris، 5 février 2014، n 12/01155.

[2] Crim. 20 mai 2015, n o 14-81.336 , D. 2015. 1466, note L. Saenko ; Gaz. Pal. 2015, n o 169, p. 8, note S. Detraz ; JCP 2015. 887, note G. Beaussonie ; CCE 2015, comm. 74, obs. A. Caprioli ; Dr. pénal 2015, comm. 123, obs. Ph. Conte ; AJ pénal 2015. 413, obs. E. Dreyer ; Dr. pénal 2015, chron. 10, obs. A. Lepage, § 15 ; Propr. intell. 2016, n o 58, p. 97, obs. M. Vivant

المقصود في المادة 311-1 من قانون العقوبات الفرنسي[1] " اختلاس غشا أموال الغير"، ولاحظت المحكمة أن البيانات المعلوماتية في جوهرها غير مادية، تشكل أموالا قابلة للتملك بطريق الغش.

إن تكييف هذا الفعل على انه سرقة، يجعله قابلا للنقد، وذلك على اعتبار أن السرقة تفرض التملك الاحتيالي، ولكن في هذه الحالة تم استخدامه للتحميل فقط، واحتفظ حامل البيانات بحرية الاستخدام، أي انه حمل المعطيات المعلوماتية وبثها إلى الغير دون أن تختلس دعامتها المادية، وبالتالي نزع الصفة المادية عن جريمة السرقة. ومن جهة أخرى يظهر انم بدا التفسير الصارم للقانون الجنائي إلى حد ما قد تم المساس به.

والسؤال الذي يطرح هنا: هل أصبحت المعطيات المعلوماتية مالا، قابل للاختلاس بطريق الغش؟

يبدو أن النقاش اختتم بالتعديل الأخير للمادة 323-3 من قانون العقوبات الفرنسي، بموجب القانون رقم 2014-1353 المؤرخ في 13 نوفمبر2014[2]، والذي وسع مجال تطبيق الدخول لنظام المعالجة الآلية للمعطيات ليشمل الأفعال، ولاسيما استخراج المعطيات بطريق الغش. وقد شدد المشرع في عقوبتها مقارنة بعقوبة السرقة، وذلك بالسجن لمدة خمس سنوات وغرامة قدرها 150،000 أورو، مقابل ثلاث سنوات سجنا وغرامة 45،000 أورو بالنسبة لجريمة السرقة.

أضف إلى ذلك، أنه قد صدر قانون جديد وهو القانون رقم 2015-912 الصادر بتاريخ 24 يوليو 2015، بحيث زاد من الغرامة المفروضة بموجب المادة 323-3 من قانون العقوبات الفرنسي من 75،000 أورو إلى 150،000 أورو.

إن السبب الذي أدى بتطبيق أحكام السرقة في قضية "Bluetouff" هو أن القانون 2014-1353 لم يدخل حيز التنفيذ بعد.

---

[1] L'article 311-1 de code pénal français dispose « Le vol est la soustraction frauduleuse de la chose d'autrui »

[2] **LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme،** JORF n°0263 du 14 novembre 2014 page 19162.(l'article 16).

ولتوضيح أكثر، إن أحكام السرقة لم تطبق في قضية نظرت فيها محكمة الجنح "Annecy"، التي صدر حكمها في 04 ديسمبر 2015[1]. وفي هذه القضية حكم على مفتش العمل وموظف في إحدى الشركات للدخول في نظام المعالجة الآلية لمعطيات المؤسسة، واستخراج بيانات الشركة تتعلق بتسريح العمال المستقبلي، ونشره في الصحافة.

فهنا لم يتم تطبيق أحكام السرقة بسبب هذا الاستخراج، بل تم الحكم بإدانة الدخول والبقاء في نظام المعالجة الآلية للمعطيات، مما يدل على عدم كفاية القانون الجنائي الذي كان موجودا قبل قانون 13 نوفمبر 2014، مما يسمح بقمع استخراج البيانات المعلوماتية.

وبالمثل ، فإن الوصول المجاني إلى المعلومات الشخصية على شبكة الكمبيوتر لشركة ما لا يقتصر على الاستيلاء الاحتيالي بأي وسيلة من وسائل الاستنساخ[2]. العقوبات التي تنص عليها المادة 323-3 من قانون العقوبات هي أعلى من تلك السرقة البسيطة ، قام المشرع باختيار عرض لحماية القيم غير المادية التي تشكل هذه البيانات.

وهكذا من الآن فصاعدا، يجب تطبيق النص الخاص للمادة 323-3 من قانون العقوبات الفرنسي[3] على سرقة البيانات المعلوماتية، وفقا لقاعدة الخاص يقيد العام «Spécialia Generalibus Dérogant ».

---

[1] Par un jugement du 4 décembre 2015, le tribunal correctionnel d'Annecy a condamné l'administrateur réseau pour accès et maintien frauduleux dans un STAD et pour atteinte au secret des correspondances. L'inspectrice du travail a, quant à elle, été condamnée pour recel de correspondances électroniques et de données internes à la société victime des actes frauduleux et pour violation du secret professionnel.

[2] Crim. 28 juin 2017, no 16-81.113 , AJ pénal 2017. 448, obs. Lasserre-Capdeville.

[3] L'article 323-3 de code pénal français dispose « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

ثانيا: موقف المشرع الجزائري من جريمة سرقة المال المعلوماتي

على اعتبار أن جريمة السرقة تقع عدوانا على الحيازة، كما قد تقع على الملكية، والمعلومات لا ترد عليها الحيازة لان لها كيانا معنويا، ذلك انه لا تتصور الحيازة إلا بالنسبة للأشياء التي يرد عليها الاتصال المادي، مما من شانه استبعاد وقوع فعل الاختلاس ذو الطبيعة المادية على محل ذو طبيعة معنوية.

وهذا كله على اعتبار أن المعلومات تختلف عن المنقولات في أنها لا تبرح مكانها بالنسخ، إذ أنها تبقى مدونة على الدعامة التي تحملها على الرغم من نسخها على شريط أو اسطوانة، ومن ثم فان اختلاسها وان كان يتسبب فعلا في دخولها في حوزة الجاني إلا انه لا يعني خروجا عن سيطرة حائزها، كل ما في الأمر انه يفقد ميزة الاستئثار بها، بينما يقتضي فعل الاختلاس في السرقة خروج المال بصورة كلية عن سيطرة المجنى عليه[1].

إن المشرع الجزائري، وبصدور القانون رقم 04-15 المعدل والمتمم لقانون العقوبات[2]، أصبحت إشكالية تطبيق النصوص التقليدية للسرقة على المال المعلوماتي موصدة، وذلك لارتباط السرقة المعلوماتية بالدخول غير المشروع لنظم المعلومات.

وهكذا يتضح أن المشرع الجزائري فرض حماية خاصة على أنظمة المعالجة الآلية للمعطيات أو البيانات في المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري.

وقد تم ذلك بتقرير جريمة الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، ومن ثم فقد جرم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات، فجرم الدخول غير المصرح به إليهما، كما جرم البقاء فيها بغير تصريح، وإذا نجم عن هذا التواجد غير المشروع داخل النظام محو أو تعديل لمعطياته فان العقوبة تتشدد[3].

---

[1] كوثر شريط، المرجع السابق، ص.395.

[2] قانون 04-15 مؤرخ في 10 نوفمبر 2004، ج ر، عدد 71، المؤرخة في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات، ج ر، العدد 49، المؤرخة في 11 يونيو 1966.

[3] تنص المادة 394 مكرر ق.ع.ج على:" يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50 ألف دج إلى 100 الف دج كل من يدخل او يبقى عن طريق الغش في كل او جزء من منظومة للمعالجة الآلية للمعطيات او يحاول ذلك.

وعلى اعتبار أن الدخول هو الركن المادي لجريمة فعل الدخول عن طريق الغش لنظام المعلوماتية، والذي يشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي والسيطرة على المعطيات التي يتكون منها والخدمات التي يقدمها[1].

وفعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية. والتقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الإلكتروني، ويقصد بالدخول أيضا الاتصال بجهاز حاسب آلي خاص بشخص الغير بدون موافقته[2].

ويتخذ الدخول صورا مختلفة؛ فمنها أن يقوم الفاعل بتشغيل جهاز مغلق وبالتالي الاطلاع على ما به من بيانات. ومنها ما يقوم به الفاعل من استخدام برامج للدخول في النظام بدون إذن صاحبه فيطلع على ما يقوم به صاحب الجهاز أو ينتقل بين أجزاء الجهاز ليطلع على ما يحتويه أقسام هذا الجهاز من معلومات.

وهكذا يقوم التجريم لفعل الدخول بغير إذن إلى نظام المعلومات، سواء كان النظام موصولا بالشبكة أم لا، وبصرف النظر عن طبيعة النشاط المتبع في الدخول، فقد يكون بالدخول المباشر إلى النظام عن طريق تجاوز جدران الحماية أو عن طريق الالتقاط الهوائي. كما أن الدخول إلى جزء من الأجزاء التي يتكون منها النظام لمعلوماتي هو بمثابة الدخول إلى النظام ككل[3].

تضاعف العقوبة إذا ترتب على ذلك حذف او تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة بالحبس من ستة اشهر الى سنتين وبغرامة 50 الف دج الى 150 الف دينار جزائري"، وتقابل المادة 6 من المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، ج.ر، العدد 57، المؤرخة في 28 سبتمبر 2014.

[1] بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة وهران، الجزائر، 2012-2013، ص.65.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة عمان، الأردن، 2008، ص.158.

[3] وسيم طعمة، المرجع السابق، ص ص.166-167.

كما أنه لم يشترط أن يتم الدخول بوسيلة أو طريقة معينة، أي أنها شاملة بكل طرق الدخول ولم تحدد طريقة بعينها[1].

وجدير بالذكر أن الدخول غير المشروع يبدأ منذ اللحظة التي يصبح فيها الفاعل قادرا على الاطلاع البصري أو السمعي لمحتويات النظام المعلوماتي[2].

إن عدم مشروعية الدخول أو ما يعبر عنه بالدخول بطريق الغش يعني الدخول غير المسموح به من قبل من له السلطة في الدخول إلى نظام الحاسب الآلي[3].

ويكون الدخول إلى النظام المعلوماتي غير مصرحا به في حالتين[4]:

1- حالة عدم وجود التصريح، بمعنى أن الشخص الذي أقدم على الدخول إلى النظام المعلوماتي، لا يحوز على تصريح يخول له القيام بذلك مطلقا.

2- حالة تجاوز حدود التصريح، وفي هذه الحالة يقوم الشخص الذي خول له التصريح بالدخول للأنظمة المعلوماتية بتجاوز الحدود التي رسمت له بموجبه، وتتم هذه الحالة عموما من طرف العاملين في المؤسسة المسؤولة عن النظام التابع لها، فهم يمتلكون عادة تصريح جزئي بالدخول يشمل مناطق محددة من النظام بحسب الوظيفة التي يؤديها كل عامل.

إن جريمة الدخول أو البقاء إلى نظام المعالجة الآلية بطريق غير مشروع، يتطلب القصد فيها علم الجاني بأنه يدخل إلى نظام المعالجة الآلية للمعطيات الخاصة بالغير، وأن تتجه إرادته إلى ارتكاب هذه الجريمة، أي أن اكتمال هذه الجريمة يستدعي توفر الركن المعنوي.

وعليه لا يتوافر الركن المعنوي إذا وقع الجاني في خطأ، كما لو كان يجهل بوجود خطر الدخول (أو البقاء)، أو كان يعتقد خطأ أنه مسموح له بالدخول[5].

الفرع الثالث: مظاهر سرقة المال المعلوماتي لدى البنوك

---

[1] بوخبزة عائشة، المرجع نفسه، ص.67.

[2] وسيم طعمة، المرجع نفسه، ص.168.

[3] وسيم طعمة، المرجع نفسه، ص.168.

[4] بوخبزة عائشة، المرجع السابق، ص ص.69-70.

[5] وسيم طعمة، المرجع السابق، ص.169.

تتم سرقة المال المعلوماتي عن طريق اختلاس البيانات والمعلومات، والإفادة منها باستخدام السارق للمعلومات الشخصية كالاسم، والعنوان، و الأرقام السرية الخاصة بالمجنى عليه، والاستخدام غير الشرعي لشخصية المجنى عليه ليبدأ بها عملية السرقة المتخفية عبر الانترنت بحيث تؤدي بالغير، إلى تقديم الأموال الالكترونية أو المادية إلى الجاني عن طريق التحويل البنكي[1].

هناك العديد من الطرق التي يلجأ إليها سارقو بيانات عملاء البنك الالكتروني للتوصل إلى هذه البيانات واستخدامها بصورة غير مشروعة، والملاحظ على هذه الطرق أنها ليست مقصورة على تعاملات العميل عبر شبكة الانترنت فقط، بل يمكن للسارق أن يتوصل إليها من خلال مراقبة نشاط العميل اليومي عامة، حتى يتسنى له التوصل إلى هذه البيانات ثم ممارسة نشاطه مع البنك عن طريق شبكة الانترنت، ومن هذه الطرق[2]:

1- قيام المعتدين بإرسال رسائل بريد الكتروني مزيفة إلى عميل البنك الالكتروني، يصورونها على أنها قادمة من البنك، حيث يطلبون في هذه الرسائل إرسال كلمة المرور الخاصة بالعميل، أو أرقام الحساب الخاصة به، ويبررون ذلك مثلا بالرغبة في حذف هذه البيانات من قاعدة البيانات الخاصة بالبنك لوجود عطل ما.

2- قيام المعتدين بتثبيت أجهزة تعمل على مراقبة سلوكيات العميل وتعاملاته مع كل الأدوات التي يمكن أن يستعملها للتواصل مع البنك، مثل الكمبيوتر الشخصي الخاص به، أو مكان سحب النقود، ويتمكن المعتدي من الحصول على هذه البيانات، إما أن يقوم بالتقاط هذه البيانات أثناء إرسالها بطريقة غير مؤمنة، أو أن يقوم بتثبيت برنامج على الجهاز الخاص بالشخص الذي يريد سرقة بياناته الشخصية، بحيث يقوم هذا البرنامج بتجميع هذه البيانات وإرسالها بصورة آلية إلى الشخص الذي قام بتثبيت البرنامج.

---

[1] مساهمة الوفد التونسي، محكمة التعقيب التونسية، الجرائم الالكترونية الواقعة على الأموال في القانون التونسي، المؤتمر التاسع لرؤساء المحاكم العليا، بيروت، 17-19 ديسمبر 2018، ص.4.

[2] علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الانترنت، دار الجامعة الجديدة للنشر، الاسكندرية، مصر، 2011، ص ص.605-607.

3- لجوء المعتدين إلى وسائل احتيالية، كإنشاء موقع الكتروني والقيام بعرض منتجات أو خدمات وهمية من خلال هذا الموقع، ويطلبون من المتعامل إدخال تفاصيل خاصة بالعميل مثل رقم حسابه المصرفي.

وبعد أن يحصل المعتدي على بيانات عميل البنك الالكتروني، فانه يقوم باستغلال هذه البيانات بما يحقق له فائدة، وعلى نحو يضر بالعميل صاحب البيانات، والتي تكون على النحو الآتي[1]:

1- التحكم في الحساب: فهنا يقوم المعتدي بالدخول لحساب العميل من خلال موقع البنك الالكتروني على شبكة الانترنت، والتعامل مع هذا الحساب باعتباره مالكا له من خلال إجراء تحويلات الكترونية لنفسه أو للغير.

2- اصطناع طلبات مزيفة: يحدث هنا عندما يقوم المعتدي بالحصول على الخدمات المصرفية من البنك الالكتروني باستعمال هذه البيانات.

في النظام المصرفي ، تغطي أنظمة المعلومات (IS) مجموعة متنوعة وواسعة التطبيقات، حيث يتكون IS من أدوات تسمح لمستشار الخدمات المصرفية لتظهر على شاشة الكمبيوتر خصائص وبيانات حسابات العملاء التي لديهم تهم، كما أنها توفر اتصالاً بالشبكة للوصول إلى جميع المعاملات المصرفية مثل استشارة الحساب ، وتاريخ المعاملات والتحويل ، والوصول إلى المعاملات غير المصرفية ، وتوفير التطبيقات الخاصة مثل معالجة المستندات وجداول البيانات، الرسومات ، محاكاة الإدارة ، إلخ[2].

ليس من الهين تأمين النظام المعلوماتي للبنوك، وأبرز دليل على ذلك النظام المصرفي السويسري، حيث بعد سرقة البيانات من البنك X. ، فتحت FINMA إجراءات ضده.

---

[1] علاء التميمي، المرجع السابق، ص.608.

[2] Marc-Eric Bobillier-Chaumon, Michel Dubois, Didier Retour. L'acceptation des nouvelles technologies d'information : le cas des systèmes d'information en milieu bancaire. Psychologie du travail et des organisations, Elsevier Masson, 2006, 12 (4), p248.

خلال التحقيق ، قامت FINMA[1] بفحص تنظيم البنك وقسم تكنولوجيا المعلومات التابع له، وظروف سرقة البيانات ومداها ، والمشاكل الأمنية لنظام تكنولوجيا المعلومات وتطويرها ، وكذلك التدابير المخطط لها لتحسين أمن تكنولوجيا المعلومات، واستند إلى معلومات من البنك وتحقيقات مستشار خارجي بتفويض من البنك.

اتضح أن السرقة تنطوي على قدر كبير من البيانات الشخصية والمالية للعملاء، واستفاد الجاني المزعوم للسرقة بشكل رئيسي من وصوله ومعرفته كموظف في قسم تكنولوجيا المعلومات بالبنك وكذلك نقاط الضعف في الضوابط ، ولا سيما من حيث إدارة الوصول وتطوير برامج الكمبيوتر.

على أساس التقارير السابقة من المراجعة الداخلية والاستشاري الخارجي ، وجدت FINMA أن تنظيم وأمن نظام تكنولوجيا المعلومات بالبنك كان يعاني ، في وقت حدوث السرقة على الأرجح ، من عدد كبير من نقاط الضعف ، والعديد منها عالية المخاطر. ثم اتخذ البنك تدابير تصحيحية كانت غير كافية لمعالجة بعض نقاط الضعف الهيكلية. منذ ذلك الحين ، اتخذ البنك خطوات إضافية مهمة[2].

تلعب تقنية المعلومات دورًا استراتيجيًا في البنوك ، بسبب تداعياتها عليها التي ستظهر فيها صعوبة و لعملائها أيضا، إذ أن المشاكل التي تمت مواجهتها كبيرة بما يكفي لتختفي البيانات أو، أخطر من اللوائح من أي نوع ولا سيما استرداد الودائع تعرض للخطر[3].

---

[1] L'Autorité fédérale de surveillance des marchés financiers FINMA (suisse).

[2] DÉCISION de l'Autorité fédérale de surveillance des marchés financiers FINMA ، Défaillances de sécurité importantes dans le domaine informatique، BULLETIN 4/2013، p.72.

[3] La France est particulièrement touchée par le vol des données personnelles. Dans son rapport publié en 2017, la société Symantec met en avant que la France est le deuxième pays le plus touché par ce fléau au monde puisque, selon son analyse, entre octobre 2015 et octobre 2016, pas moins de 85,3 millions d'éléments d'identité (des simples noms et prénoms à l'adresse en passant par les mots de passe) ont été volés en France. La France se situerait juste derrière les USA et devant la Russie. La négligence des

تظل سرقة البيانات الشخصية (خاصة في ملفات العملاء) هدفًا للاقتحام في أنظمة معالجة البيانات الآلية. يتم إعادة استخدام البيانات التي تم الحصول عليها إما للعمليات الاحتيالية التي تستهدف عملاء محددين ، للابتزاز على حساب الشركة ، أو بيعها ، لا سيما في المنتديات المتخصصة أو الشبكات الوهمية[1].

من وجهة نظر جوهرية ، يتألف الاستخراج الاحتيالي للبيانات الواردة في نظام المعالجة الآلية للمعطيات من البحث عن البيانات الشخصية (مثل عناوين البريد الإلكتروني ورقم البطاقة المصرفية) في قاعدة البيانات ، باستخدام الوسائل التقنية (على سبيل المثال ، النص البرمجي أو البرامج الضارة) مما يسمح باستخراجها بطريقة احتيالية أو غير قانونية[2].

هذا هو الحال عندما يقوم أحد المواقع بجمع بيانات شخصية بشكل غير عادل باستخدام مخطوطات أو روبوتات لجمع البيانات وتحديدها ، وخاصة لغرض معرفة ما إذا كان العميل نشطًا على الموقع أم لا ، ووضع وسيلة فنية لاستخراج البيانات التي تم جمعها من أجل تغذية موقعها المنافس ، ثم على الرغم من أن الشروط العامة للموقع تنص بوضوح على أن هذا الإجراء محظور تحت طائلة الإجراءات القانونية [3].

أما فيما يتعلق بالاحتفاظ بالبيانات ، فقد يكون هذا أقرب إلى تلقي البيانات المستخرجة أو المستنسخة أو المنقولة بطريقة احتيالية، وهنا يتعلق الاستنساخ الاحتيالي للبيانات بأفعال النسخ، أيا كانت الوسيلة ، فإن مصطلح "الاستنساخ" يسمح بتكييف بعض الأحكام القانونية مع الرقمية.

---

internautes en matière de cybersécurité explique la majorité des piratages. Un internaute sur deux continuerait de répondre aux mails de phishing.

[1] LA RÉPONSE DU MINISTÈRE DE L'INTÉRIEUR française، Thierry DELVILLE Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces، ÉTAT DE LA MENACE LIÉE AU NUMÉRIQUE EN 2018، Rapport n° 2، Mai 2018، p. 48

[2] Frédérique CHOPIN، Cybercriminalité، Répertoire de droit pénal et de procédure pénale، Dalloz، janvier 2020،37.

[3] Paris, Pôle 4, ch. 11, 15 sept. 2017, M. X c/ Weezevent.

أخيرًا ، يهدف نقل البيانات إلى أي شكل من أشكال نشر البيانات إلى طرف ثالث ، مهما كانت الوسيلة. أما بالنسبة للعنصر الأخلاقي ، فنجد هنا شرط التصرف "بشكل احتيالي" ، كما كان من قبل فيما يتعلق بإدخال البيانات[1].

والجدير بالذكر، يعد الأمن ومكافحة الجرائم الإلكترونية من التحديات الرئيسية للقطاع المصرفي على أساس أن العلاقة بين البنك وعميله هو الثقة ، ومن الضروري الحفاظ عليه من خلال تطبيق جميع الوسائل اللازمة لأمن المعلومات.

في هذا السياق ، قرر الاتحاد المصرفي الفرنسي (FBF) والمديرية الفرعية لمكافحة الجرائم السيبرانية (SDLC) للشرطة القضائية التوقيع على شراكة، هذا التعاون هو جزء من نهج أوروبي من قبل يوروبول والاتحاد المصرفي الأوروبي الذي يهدف إلى تعزيز مكافحة الجرائم الإلكترونية.

الخاتمة

إن التقنية الحديثة سهلت ظهور طائفة جديدة من الجرائم المستحدثة من بينها جريمة سرقة المال المعلوماتي عبر الانترنت، والتي تعجز النصوص العقابية التقليدية على مواجهة أغلب صورها، وإن وجدت نصوص عقابية حديثة فلابد أن تكملها استراتجيات وذلك لمراقبة الأمن في نواحي مختلفة على المستوى الفني والتقني والقضائي مجال تقنية المعلومات.

لقد تدخل المشرع الجزائري بسد الفارغ القانوني الموجود و إصدار تشريع قانوني خاص بجريمة سرقة المال المعلوماتي عبر الانترنت متجاوزا هذه التسمية للخصوصية التي يتميز بها المال المعلوماتي، هذا المجال سعت لسده في باد ئ الأمر بتعديل قانون العقوبات 04-15، و لكن محدودية هذا القانون دفع المشرع الجزائري إلى إصدار قانون خاص والمتمثل في القانون رقم 09-04و المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتخليه على حرفية النص الجنائي وتبنيه مفهوما أشمل للمال و المنقول، بحيث شمل الأموال المعلوماتية المعنوية.

وهكذا، لا يمكن تطبيق أحكام سرقة المال المعلوماتي من خلال النصوص التقليدية للقانون الجنائي، إلا من خلال سرقة الدعامة المادية[2]. وأن أي اختلاس للمال المعلوماتي سواء بطريق

[1] Frédérique CHOPIN. Op.cit، 38.

[2] CA. Grenoble, 1ère chambre correctionnelle, 4 mai 2000

المشاهدة أو أي وسيلة من هذا القبيل يخضع لجريمة الدخول إلى نظام المعالجة الآلية للمعطيات بطريق الغش.

الإرهاب الالكتروني نمط للاأمن المعلوماتي

Electronic terrorism is a pattern of no information security

د. زروال معزوزة أستاذة محاضرة أ
كلية الحقوق و العلوم السياسية
جامعة أبي بكر بلقايد تلمسان الجزائر

د. بلغازي نور الدين أستاذ مؤقت
كلية الحقوق و العلوم السياسية
جامعة أبي بكر بلقايد تلمسان
الجزائر

مقدمة

تعميم استعمال الحواسيب رتّب يقينا ايجابيات تخص اقتصار الزمن و المسافات و تقريب الخدمات، و انجاز العمليات التجارية الأكثر حساسية بفضل تكنولوجيات الاعلام و الاتصال الذي عنوانه الرئيسي الانترنت أو المصطلح الرائج ألا و هو العالم الافتراضي .

أمام هذه المستجدات التكنولوجية الرافدة إلى المعاملات البشرية ، بات ضروريا وضعُها في حيزها القانوني تلافيا للتجاوزات خاصتها ، و قبلها ضبط شروط استخدام هذه الوسائل في المعاملات مهما كانت طبيعتها[1].

فالمعلومة متاحة للجميع و آثار انحراف استعمالها أصبحت مباحة في ساحات الحروب والمشاحنات الالكترونية المتحرّرة من القيد الزماني و المكاني ، و نَمَا الشعور بالحقد و الكراهية والتطرف . وتوسَّعت سُبل الاتصالات إلى تكوين مجاميع و منظمات تعتمد على ما توفره و سهّله التقنيات الحديثة الناشطة في شتى المجالات، سيما المنظمات الارهابية الخدومة لتجنيد المواطنين و تدريبهم[2].

---

[1] - مختار الاخضري ، "الاطار القانوني لمواجهة جرائم المعلوماتية في الفضاء الافتراضي" ، مجلة الجريمة المعلوماتية، مركز البحوث القانونية و القضائية ، الجزائر ، ص 51

[2] - فريج سعيد العوضي ، حروب تقنية المعلومات ، طبعة 1 ، دار العلوم العربية للنشر و الاعلام ، مصر ، ص 13.

وفإن كانت الجريمة بمعناها التقليدي تعني كل فعل أو خروج عن السلوك أو المعايير الاجتماعية و الثقافية و الاقتصادية التي يحكمها القانون الوضعي لأي مجتمع [1]، اتسعت السياسة الامنية باعتمادها مقاربتي الأمن الانساني و الأمن الشامل في رسم مختلف السياسات الوطنية، وإحكام التدابير الحكومية الرامية إلى مواجهة مختلف التهديدات و الاخطار المستحدثة سيما المعلوماتية ، بتنوع مستويات و طبيعة مهدداتها المتمثلة في حماية السيادة ، الاقليم الوطني ، مكافحة الارهاب ، الاصلاحات السياسية ، السياسات الاجتماعية[2].

مع تنامي الاستعمالات التكنولوجية و انفتاح العالم بفضل النظام المعلوماتي كثورة حضارية ، تيسّرت المعاملات بين الافراد و المجتمعات و الدول ، كما تعاظمت في ذات الوقت الجرائم من ذات الجنس الالكتروني بين الاختراقات و التجسّس إلى الارهاب المستعين بالفضاء الافتراضي.

و قد عرفت الجزائر أكثر من 100 جريمة الكترونية سنة 2014 ليتضاعف هذا العدد خلال السداسي الاول من سنة 2015 إلى أكثر من 200 جريمة الكترونية ، يتعلق ابرزها بانتهاك الحريات الشخصية و التهديد عبر الانترنت ، و نشر صور فاضحة ، الابتزاز و القرصنة الالكترونية و غيرها [3].

على أن الارهاب الالكتروني يعد من اخطر الجرائم المعلوماتية لتأثيره المدمّر للبشرية إقتصاديا و إجتماعيا و نفسيا ، علاوة على أنها تدير حربا بين الدول المتطوّرة تكنوجيا ، و ليس للدول النامية سوى أن تكون مخبرا للتجارب في غالب الاحيان .

لذلك كان على السياسة الأمنية في الجزائر أن تؤطر قانونها العقابي ليتناسب مع هذه التطورات و التعاملات المعلوماتية، للحد من الافعال المسيئة للتقنية و متابعة مرتكبيها بطرق أكثر حداثة.و تعاونها دوليا بالمشاركة في جميع الاتفاقيات الموحّدة للقواعد الاجرائية لمتابعة الجرائم المعلوماتية عامة و الارهاب الاكتروني خاصة ، و التعامل الفطن في الداخل من خلال التدخل التشريعي الصارم ، و التكوين المستمر للهيئات المتخصّصة في مكافحة هذه الجرائم .

---

[1] -حسنين شفيق،الاعلام الجديد و الجريمة الإلكترونية-التسريبات-التجسس الالكتروني-الارهاب،دار فكر و فن للطباعة و النشر و التوزيع، مصر،ص 182

[2] - منصور لخضاري،السياسة الامنية الجزائرية،المحددات - الميادين - التحديات، المركز العربي لابحاث ودراسات سياسية ، قطر، ص 04

[3] -بن مرزوق عنترة و الكر محمد ،" البعد الالكتروني للسياسة الامنية الجزائرية في مكافحة الارهاب" ، مجلة العلوم الجتماعية و الانسانية ،المجلد 19 ، العدد 1 ،ص 10.

مدخل تمهيدي : تداعيات التقنية و الفكر الامني الجديد

يعد التعامل مع العالم الافتراضي بمكوناته المتشابكة أرقى مظهر للدول المتطورة تكنولوجيا، و تصنيف جديد لمجتمعات القوية اقتصاديا و عسكريا و تقنيا . و في ذات الوقت أعطى مفهوما حديثا للفكر الامني الذي تخطى الحدود السيادية للدول .

أ- الزخم التقني و الجرائم الالكترونية

التطور الكبير و المتسارع لشبكة الانترنت صاحبه ظهور جرائم مستحدثة ما كانت لتظهر لولا الشبكة المعلوماتية ، و اصبحت هذه الاخيرة موطنا للكثير من الأعمال الأجرامية للاسباب التالية :

- لا مركزية المعلومة المتداولة عبر الفضاء الالكتروني ، و ليس هناك تنظيم دولي موحّد في تأطير الجرائم المتوّلدة عن هذا الحدث التقني .
- القصور الاجرائي في التحقيق لهذا النوع من الجرائم ، لنقص الخبرة لدى الشرطة القضائية و القضاة سيما في مسألة التقصي عن الادلة .
- تخطي الحدود الزمنية و المكانية للجرائم الالكترونية صعَّب من عملية اكتشافها[1].

وقَّع هذا التطور السريع للتكنولوجيا بصماته في عديد القطاعات الحيوية مثل المواصلات و التعاملات المالية ، و قطاع الطاعة و قطاع الاتصالات و اقترن بالتوازي مع التطور السريع في تقنية الحواسيب و المعلومات و الشبكات ، و فتح المجال واسعا امام الارهاب الدولي خصوصا، و مكّنه من الوصول إلى مكونات البنية التحية المُسيّرة تقنيا ، ببرامج و آلات و أدوات مُكَننة.[2]

إذن ايجابيات التواصل و الاتصال الالكتروني و خدماتها الجليلة، في بعث نفس جديد للهيا كل الاساسية تكون مقيدة بعدم إضعاف جهازها الامني من خلال إساءة استعمال تقنيات المعلومات لضرب المقومات الحيوية للدول ، أو المساس بالحريات و الحقوق الأصيلة للأفراد ،

[1] - غادة نصار ، الارهاب و الجريمة الالكترونية ، دار العربي للنشر و التوزيع ، قصر العيني ، مصر ، ص 14 .

[2] - مصطفى يوسف كافي ، جرائم الفساد-غسيل الاموال-السياحة-الارهاب الالكتروني-المعلوماتية ، الطبعة الولى ، مكتبة المجمع العربي للنشر و التوزيع ، عمان ، 2014 ، ص 165 .

لنكون أمام ما يصطلح عليه بالجرائم الالكترونية التي تهدّد سرية المعلومة و تؤثر على أمنها من حيث الحفظ و التخزين [1].

إن شبكة الانترنت تخزان معلوماتي له ابعاد ثلاث و هي سرية المعلومات و سلامتها ووجودها ، استتباعا لذلك وجب التامين على المعلومات المتنقلة في العالم الافتراضي [2].

فيكون من الاهمية بمكان إعادة النظر في مفهوم الامن ذاته ، من النظرة التقليدية المرادفة لمكافحة الجريمة إلى مقاربات تخص التطوير التقني و الرقي التكنولوجي لحل عقد الجرائم المتفشية عبر الفضاء الالكتروني.

و مهما كانت الاسباب و التعريفات و المعتقدات ، فحقيقة الامر أن البنية التحتية العالمية مهددة ، و الاختراقات و العبث بالمعلومات المخزنة أو المتداولة من خلال شبكات الاتصال في تزايد مستمر لأهداف و مسببات عدة .

ذلك ان خدمات البنية التحية في العالم تعتمد إلى حد كبير و بأسلوب متزايد على شبكات نقل المعلومات من شبكة الاتصالات التي تشمل الكوابل المحورية و الاتصالات الفضائية والهواتف الثابتة و النقالة ، و شبكات لنقل الطاقة ، و تشمل شبكات الكهرباء و أنابيب الغاز و انابيب نقل النفط . و جميع هذه الشبكات مُمكننة في غالبيتها ، و تتجه نحو مزيد من الاعتماد على التحكم الحاسوبي لتنفيذ جميع وظائفها التشغيلية ، مما جعل احتمالية تعرضها للأعطال والتخريب عالية جدا .

و بالتالي يكون الخطر محدقا بموارد الطاقة و الثروات المُقادة بتقنيات تكنولوجيا المعلومات لأنها غير محصنة بالقدر الكافي من الهجومات و الاختراقات اللاّمسؤولة [3]. فالتخوفات من تعطل البنى التحتية بعامل الافعال المنحرفة للتقنية أبان على فقدان الدولة لسيطرتها في التعامل

---

[1] - مصطفى يوسف كافي ، الادارة الالكترونية ، دار و مؤسسة رسلان للنشر و التوزيع ، عمان ، 2011 ، 13 .

[2] - أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الانترنت ، دار المطبوعات الجامعية ، 2008 ، الاسكندرية، مصر ، ص 124 . و انظر كذلك اسماعيل عبد الحكيم بكر ، المعلوماتية قوة اقتصادية ، العربي للنشر و التوزيع، مصر ، ص 70 .

[3] - لينا جمال محمد ، الجرائم الالكترونية ، دار دار خالد اللحياني للنشر و التوزيع ، عمان ، 2016 ، ص 16 .

منفردة مع الظاهرة ، و حثها على الاجتهاد دوليا لخلق ضوابط حامية للمصالح المشتركة المهددة ،بالتشارك مع المنظمات و المؤسسات الراعية للفكر الأمني في عالم المعلوماتية [1].

ب/ نمو الجريمة الالكترونية

ان التطور المعلوماتي مظهر راقي للدول و يدخل ضمن سياستها التخطيطية في المعالجة الذكية للجرائم المنبثقة عنها ، سواء في المعاملات الاقتصادية أو ما تعلق بالجانبين الامني و السياسي لعوامل لها شأن بالتدفق السريع للمعلومة ، و خرق قواعد الزمن و المسافة . الأمر الذي سرّع من اختراق الحدود الأمنية للدول و شجّع على تجميع الجهود في توحيد السيادة القانونية لمكافحة الارهاب في العالم الافتراضي . فالانفراد بالحلول لا يوفّر حماية للدول أو المواطنين في عالم الرقمنة، أين يكون صنع آلات عسكرية حديثة مبنية على وسائل الاتصالات الحديثة و المنظومة الاستخباراتية و التجسسية ، مهما كان الهدف المرصود ، فيكون من العبث تحديد القيم أو الأنظمة المراد تدميرها [2].

- **تقنية تعريف الجريمة الالكترونية**

هي الخليط المتجانس لأفعال غير مسؤولة لاستعمال التقنيات الحديثة و المتصلة اتصالا وثيقا بالحاسب الآلي و بنظام المعلومات [3] .

و يمكن تعريفها بأنها الافعال الاجرامية التي تتم في العالم الافتراضي عن طريق المساس بقواعد الامن الخاصة بالمعلومة المتداولة إلكترونيا ، و من أمثلتها الارهاب الالكتروني و غسيل الاموال و الجوسسة الالكترونية .

و يكون من المهم التمييز بين جرائم الحاسب الالي و جرائم الانترنت ، ففي الحالتين المجرم يتمتع بسمات و صفات عالية و له دراية كاملة و خلفية معرفية متقدمة بأنظمة تشغيلها ، كما يقتربان في صعوبة اكتشافهما . بينما تختلف الجريمتين في أن ارتكاب جرائم الانترنت يشترط وجود حاسب آلي متصل بالانترنت لاتمام أركان الجريمة ، أما جريمة الحاسب لا تحتاج الى

[1] - نبيل عبد الفتاح ، الارهاب الالكتروني القوة في العلاقات الدولية نمط جديد و تحديات مختلفة ، الطبعة الاولى ، مطبوعات مركز الدراسات السياسية و الاستراتيجية ، القاهرة ، 2009 ، ص 50

[2] - فرحان فرع العتيبي ، المعلوماتية و أثرها على النظم العربية ، مكتبة مجمع العربي للنشر و التوزيع ، عمان ، ص 15

[3] - اسماعيل عبد الحكيم ، المعلوماتية قوة اقتصادية ، العربي للنشر و التوزيع ، 2012 ، مصر ، ص 87 .

وسيلة الربط كما هو الحال في جرائم التزييف و التزوير و سرقة المعلومات و تدميرها ، ثم إن الصبغة الدولية تكون السمة البارزة في جرائم العالم الافتراضي [1].

- **تميُّز الجريمة المعلوماتية**

- اعتلاء الفكر التقني المتقدم مظهر بارز في كل مرحلة من مراحل ارتكاب الافعال في النظام المعلوماتي [2].
- دولية الجريمة الالكترونية و اقلاق السيادة القومية للدول بسبب اختزالها للزمان والمكان و سرعة تداول المعلومات الموجهة لافعال مسيئة للتقنية و المعلوماتية [3].
- تعدد المشاركين في ارتكاب الجرائم الالكترونية بين الافراد و المنظمات و الدول ، و عدم القدرة على تحديد الاهداف المقصودة بالضرب الالكتروني و لا حتى الاسباب التي تتنوع بين الدولفع السياسية و الدينية و الايديولوجية .
- سرعة العمل الاجرامي الالكتروني و دقته و تغييب الادلة باستعمال نفس الوسيلة الجرمية عقد عملية التحقيق فيها و اكتشافها و بالتالي الحد من آثارها .
- آثار ارتكاب الجرائم مكلفة ماديا و نفسيا فهي تمس قواعد حيوية متمثلة في ضرب البنى التحتية ، و تخلف آثارا نفسية كلما اساءت للحريات و الحقوق الاساسية للافراد و المجتمعات و تحد من ممارستهم الطبيعية لها .

لذلك تعمل التنظيمات الارهابية بشكل مستمر على مثالية استخدام وسائل المعلومات الالكترونية المتطورة ، و ما يشجعها توافرها على عناصر السرية بين المتعاملين به أولا و تدفق المعلومات باستمرار و ثانيا للانخفاض الكبير في أسعارها و سهولة الحصول عليها و اخيرا القدرة الميسرة في الاتصال بالجماهير و حشدهم [4].

البند الاول : الارهاب الالكتروني الظاهرة الاجرامية

---

[1] - محمد علي سكسكر ، الجريمة المعلوماتية و كيفية التصدي لها http:// www.eltahrir.net

[2] - مروان بن مرزوق الروقي ، القصد الجنائي في الجرائم المعلوماتية – دراسة تاصيلية مقارنة -، الطبعة الأولى، مكتبة القانون و الاقتصاد ، الرياض ، 2013 ، ص 17

[3] - فرحان فرع العتيبي ، المرجع السابق ، ص 22 .

[4] -خالد مرزوق سراج العتيبي،الجوانب الاجرائية في الشروع في الجرائم المعلوماتية–دراسة مقارنة-،مكتبة القانون والاقتصاد،الرياض،ص 144

لاقت جرائم الارهاب الالكتروني اهتماما عالميا، فعقدت المؤتمرات و الندوات المختلفة لتناول الظاهرة و تأطيرها بغرض مواجهتها ، ذلك أن الارهاب من هذه الفصيلة يتميز بمجموعة من السمات تُصعّب مهمة المحققين لأنها متعدية الحدود و القدرة على طمس الدليل .

أ/ الاطار المفاهيمي لجريمة الارهاب الالكتروني

ان كان الارهاب بصفة عامة هو ذلك السلوك الاجرامي الذي سبب قدرا كبيرا من الدمار و الخسائر البشرية ، و ينفذه جماعات متخصّصة من ذوي الخبرات العالية التي تمتلك معرفة تكنولوجية في مجالات متعددة و لها قدرة عالية على التخطيط[1] . فإن مفهوم ان مفهوم الجريمة الارهابية التقنية يمكن تحديدها بانها :" أي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ العمل الارهابي"[2].

و ينطلق الارهاب بجميع أشكاله و شتى صنوفه من دوافع متعددة و يستهدف غايات معينة[3].

و ليست اللغة العربية بعيدة عن المعنى الاصطلاحي في التعريف بالإرهاب عامة في انه تعبير عن الترهيب و التخويف .و هو ما انتهى إليه مجمع الفقه الاسلامي التابع لرابطة العالم الاسلامي شمولية في العناصر الخاصة بالإرهاب بأنه :" العدوان الذي يمارسه أفراد أو جماعات أو دولا بغيا على الانسان ، دينه ، و دمه ، و عقله ، و ماله ، و عرضه ".

و بالتالي هو فعل ينطوي على تعنيف أو تهديد ، مردّه خطة جماعية أو فردية لبعث الريبة و الجزع في الأنفس ، و النتيجة تهديد أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر ، سواء مسّت هذه الافعال البيئة أو مواردها ، و سواء تعلق الامر بالاملاك العامة أو الخاصة [4].

الارهاب الالكتروني يكون له نفس مقاصد التهديد و الخطر المهوّل لأحوال الناس وبعث الرهبة في نفوسهم ، باختلاف الوسيلة المتمثلة في استخدام الوسائل الالكترونية و اتصال الدول

[1] - حلمي النمر و هويدا مصطفى ، الاعلام و التنمية في مواجهة الارهاب .العربي للنشر و التوزيع ، مصر، ص 53

[2] - حسنين شفيق ، المرجع السابق ، ص 183

[3] -نعوم تشومسكي ، ثقافة الارهاب ، نقله إلى العربية محمود صالح محمد منذر ، الطبعة الاولى ، العبيكان للنشر، الرياض ، 2016 ، ص 87

[4] - قرار مجمع الفقه الاسلامي الدولي ، الدورة 14 ، منعقدة بالدوحة في شهر ذي القعدة عام 1423 .

أو الجماعات أو الافراد عبر الفضاء الافتراضي [1]. لتكون التقنيات الرقمية الاساس للهجمات الارهابية مهما كان المخطط الرامي إلى ضرب الحريات الاساسية .

يمكن تعريف الارهاب الالكتروني انطلاقا مما سبق بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الافراد باستخدام الموارد المعلوماتية والوسائل الالكترونية[2]

او هي الاعتداءات غير المشروعة أو التهديد بها الواقع على المعلومات المتداولة في الفضاء الالكتروني المتصلة بالحاسبات الآلية ، من أجل الانتقام أو المساومة على قضية معينة أو للتأثير على الحكومات أو المجتمع الدولي بأسره ، لدوافع متعدّدة قد تكون ايديولوجية أو سياسية أو اقتصادية . ليترتب على هذه الافعال إلحاق أضرار بالأشخاص و الممتلكات العامة و الخاصة أو على الاقل تحدث أذى كافي بنشر الخوف و الرعب [3].

و مع ذلك ليس هناك مفهوم دولي موحد للإرهاب بصفة عامة و الارهاب الالكتروني بصفة خاصة و لا حتى جهود واضحة لتحقيق هذه الغاية [4].

ان اللغط الكبير في تقديم شرح لمفهوم الارهاب الالكتروني صعّب تطبيقات مواجهته بسبب اختلاف السياسات المنتهجة من طرف بعض الدول لتحقيق مآربها ، مثلما وضعت الو.م.ا حركات التحرر ضد العدو الاجنبي و وصفتها بالأعمال الارهابية .

و قد عرّفه قاموس لاروس بانه مجموعة من الهجمات الخطيرة (فيروسات ، قرصنة...الخ) على الحواسيب ، شبكات و انظمة الاعلام الآلي لمؤسسة أو هيئة ، ترتكب لخلق فوضى عامة تهدف بعث الرعب . و عرّفه قاموس كورديال بأن مجموعة من الهجمات على شبكة الانترنت باستخدام الفيروسات و البرامج المخرّبة للبيانات . على أن التعريف الاخير لم يحدد

---

[1] - عادل عبد الصادق ، الارهاب الالكتروني نمط جديد و تحديات مختلفة ، المركز العربي لابحاث الفضاء الالكتروني ، 2013 ، ص 171

[2] - مصطفى يوسف كافي ، جرائم الفساد – غسيل الاموال – السياحة – الارهاب اللالكتروني – المعلوماتية - ، المرجع السابق ، ص 143 .

[3] - بن عمر عوينات ، "الارهاب الالكتروني : المفهوم و الجهود الدولية و الاقليمية لمكافحته" ، مجلة الاستاذ الباحث للدراسات القانونية و السياسية ، العدد 6 ، 2017 ، ص 36 .

[4] - أمير عبد العزيز العربي و محمد عبد المنعم كامل ، جذور الارهاب و آليات المواجهة ، الطبعة الاولى ، أطلس للنشر و الانتاج و الاعلام ، الجيزة ، مصر ، 2019 ، ص 10

الاهداف من الافعال الجرمية،و ان كان قد بين أن محرّك الاجرام محترف ذوي كفاءة عالية في مجال تقنية المعلومات لضرب أهداف عسكرية أو مدنية [1].

ب/المفاهيم المتداخلة مع الارهاب الالكتروني

هناك فرق بين الإرهاب الالكتروني و الأعمال الارهابية التي تمارس على شبكة الانترنت، فعرف الارهاب الالكتروني بأنه كل الانشطة التي يقوم بها أفراد او جماعات باستخدام النظام المعلوماتي قصد إحداث دمار بالبنية التحية المسيرة بواسطة نفس الاداة الالكترونية. بينما عرفوا الاعمال الارهابية التي تمارس على شبكة الانترنت بأنها الأنشطة التي تقوم بها منظمات أو جماعات ارهابية تقليدية من أجل تحقيق إجرامها في الميدان ، و تشمل أنشطة التجنيد ، الدعاية، المواد التعليمية الخاصة بالأعمال الارهابية ، تبادل الاوامر ...ألخ .[2].

و في الحقيقة ليس هناك أي فرق بين الارهاب الالكتروني و حرب المعلومات ، و يقصد بالعبارة الاخيرة استخدام نظم المعلومات لاستغلال و تخريب و تدمير و تعطيل معلومات الخصم بحيث تصبح أداة ارهابية لتنفيذ أهدافهم بغض النظر عن محركها أن كانت دولا او منظمات أو افرادا . و أن كانت الحرب في معناها الشامل تكون في الغالب الاعم بين الدول المتصارعة اقتصاديا أو ايديولوجيا[3] .

و قد يقوم الخلط بين الارهاب الالكتروني و حرية التعبير، ذلك أنه من ثمار التكنولوجيا المساهمة في بناء ديموقراطية رقمية جديدة تسهل عملية الوصول الى صانعي القرار و المشاركة السياسية حتى تكون فعّالة ، و تيُسّر عملية الوصول الى المعلومة . سيما أن طبيعة الاتصال الالكتروني تحولت من مجرد تواصل بين النخبة الى فسحة تحاور و تشاور بين الطبقة الرائدة والجماهير العريضة في الداخل و الخارج .

---

[1] - توفيق مجاهد و طاهر عباسة ، "جريمة الارهاب الالكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010" ، مجلة العلوم القانونية و السياسية ، المجلد 9 ، العدد 3 ، 2018 ، ص 81

[2] - كما عرفه مركز حماية البنية التحتية القومية الامريكية بانه "كل عمل اجرامي يتم التحضير له عن طريق استخدام أجهزة الكمبيوتر و الاتصالات السلكية و اللاسلكية ، ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف ارباك و زرع الشك لدى السكان للتاثير عليهم او على الحكومات خدمة لاجندة سياسية أو اجتماعية أو ايديولوجية" توفيق مجاهد و طاهر عباسة ، جريمة الارهاب الالكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقية المعلومات لعام 2010 ، مجلة العلوم القانونية و السياسية ، المجلد 9 ، العدد 3 ، ديسمبر 2018 ، ص 18

[3] - عادل عبد صادق ، المرجع السابق ، ص 137

و كانت الحركات الدينية و السياسية لها السبق في الاهتمام بالانترنت بسبب طبيعتها السياسية الساعية إلى نشر أفكارها بطريقة سريعة و كسب اكبر عدد من المؤيدين . الامر الذي قد يترتب عليه تفاعل بين مفهومي الارهاب و حرية التعبير حين تستغل الجماعات الارهابية المنتديات الالكترونية في التنظيم لأعمال العنف .

تعدّدت التعريف الخاصة بالإرهاب الالكتروني، على أنها كلها تتفق في أنه استخدام شبكات المعلومات و أجهزة الكمبيوتر المتصلة بالانترنت بغرض التخويف و الارغام لتحقيق أهداف سياسية أو اقتصادية او ايديولوجية .كما أن هناك فرقا بين الارهاب كظاهرة إجرامية ، و الإرهاب كظاهرة قانونية . فالظاهرة الاجرامية تستمد طبيعتها من تأثيرها في المجتمع و هي تعالج بوسائل مختلفة منها الوسائل الأمنية و الاجتماعية و القانونية ، و ترتبط بالبواعث أو الاسباب التي تؤدي إلى الارهاب . كما ترتبط بتأثيرها في الاستقرار و الأمن الداخلي و الأمن و السلم الدوليين فضلا على مساسها بقيم الديموقراطية و حقوق الانسان [1].

و تحدّد الظاهرة القانونية في ضوء ما يراه القانون الدولي لضبط أحكام الظاهرة الاجرامية بتحديد العناصر الخالقة لأركان التجريم .

ج/ تعريفات الاتفاقيات الدولية

عرفت الاتفاقية الدولية لمكافحة الارهاب المنعقدة في جنيف لعام 1973 الارهاب على انه فعل اجرامي موجه ضد احدى الدول و هدفه اثارة الفزع و الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة .

و عرفته الاتفاقية الدولية الاولى لمكافحة الاجرام عبر الانترنت في بودابست عام 2001 على :" هجمات غير مشروعة أو تهديدات بهجمات ضد الحواسيب أو الشبكات أو المعلومات المخزنة الكترونيا ، توجه من أجل الانتقام أو الابتزاز أو الاجبار أو التاثير في الحكومات أو الشعوب الدولي بأسره لتحقيق اهداف سياسية أو دينية أو اجتماعية معينة "[2].

---

[1] - عبد الحميد معتز محيي ، الارهاب و تجديد الفكر الامني ، الطبعة الاولى ، دار زهران للنشر و التوزيع ، عمان ، 2014 ، ص 07

[2] - سعيد عبيدي ، "الارهاب الالكتروني "، مجلة العلوم الانسانية ، المركز الجامعي تندوف ، العدد 2 ، سنة 2017 ، ص 13

و عرفه الاتحاد الاوروبي بعد العام 2002 بانه " عمل اجرامي هدفه ترويع الناس أو اجبار الحكومات أو الهيئات الدولية على القيام بعمل أو الامتناع عن القيام به ، أو تدمير الهياكل الاساسية الدستورية ، الاقتصادية و الاجتماعية للدولة أو الهيئة أو زعزعة استقرارها"[1].

يبدوا واضحا أن التعريف بهذه الظاهرة أخذ منهج البحث في عناصر الجريمة و أهدافها للتعرف عليها ، المسألة التي خلقت ارتياحا لدى مرتكبي هذه الجرائم في ظل التشتُّت المفاهيمي لهذه الجريمة و عَسَّر من مواكبة الافعال المسيئة لنظام المعالجة الآلية للمعلومات .

للدول العربية بادرة جادة في تكثيف جهودها لمواجهة الآثار السلبية لهذه الجريمة ، الامر الذي أثمر في البيان الختامي الصادر عن الدورة 09 لوزراء الخارجية للدول العربية و الاسلامية المنعقد في الدوحة في العاشر من اكتوبر من العام 2001 ، و تحت رعاية منظمة المؤتمر الاسلامي[2].

أما الاتفاقية العربية لمكافحة الارهاب لسنة 2010 في الفقرة 2 من المادة الاولى عرفت الارهاب بأنه " هو كل فعل من أفعال العنف و التهديد به أيا كانت بواعثه أو أغراضه ، يقع تنفيذا لمشروع اجرامي فردي أو جماعي ، و يهدف إلى القاء الرعب بين الناس و يعرض حياتهم او حرياتهم او أمنهم للخطر أو الحاق الضرر بالبيئة أو باحد المرافق أو الاملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر[3].

إن هذا النوع من الارهاب الحديث يتم فيه نشر الافكار و المعتقدات ، و من تم يتم التخطيط و التجهيز للعمليات الارهابية ، ثم التنسيق و التبادل بالمعلومات و كشف مواقع تعليم صناعة المتفجرات و الالغام و الاسلحة الكيماوية الفتاكة فضلا عن طرق و آليات اختراق و تدمير المواقع و البيانات و النظم المعلوماتية و دخول المواقع المحجوبة و أعمال التجسس و طرق نشر الفيروسات مع مواقع تهدف إلى شنّ حملات نفسية على الدول و المجتمعات .

د/ دراسة بعض الحوادث الخاصة بالإرهاب الالكتروني

---

[1] - أمير فرج يوسف ، المرجع السابق ، ص 167

[2] - عبد الله عبد العزيز العجلان ، الارهاب الالكتروني عي عصر المعلومات ، العربي للنشر و التوزيع ، القاهرة ، مصر ، ص 13 .

[3] - علي عدنان الفيل ، الاجرام الالكتروني ، الطبعة الاولى ، مكتبة زين الحقوقية و الادبية ، صيدا ، لبنان ، 2011 ، ص 56 .

الأمم المتحدة لم تعالج حتى الآن أية حالة يمكن الاستناد اليها في تعريف الارهاب الالكتروني و امكانية التعامل معه من الناحية القانونية او الجُرمية ، ثم إن القانون الدولي عامة لم يعط تعريفا واضحا و منهجا معينا للتعامل مع هذا النوع الجديد من الارهاب .و لابد من الاشارة أن قضية الحرب على سوريا فرضت على مجلس الامن التعامل مع هذا الوضع، سيما أن العمليات المقصودة استخدمت فيها تكنولوجيا المعلومات[1] .

و من الامثلة على الهجمات الاقتصادية العملية التي قامت بها مجموعة من الهاركز ، تعرف باسم نادي الفوضى عام 1997[2] لتحويل الاموال المصرفية . او ما حدث في مارس سنة 1995 من هجوم على ميترو الانفاق في طوكيو [3]. وكذلك تفجيرات مدينة ممباي في العاصمة الاقتصادية في الهند في 26 نوفمبر و التي ادت إلى مصرع 195 شخص و جرح 300 آخرين [4].

البند الثاني :عناصر الجرائم الارهابية الالكتروني

دراسة الظاهرة الاجرامية التي عنوانها الارهاب الالكتروني يفرز عن تدخل عنصرين في تكوينه هما :

أ/ المجال المعلوماتي :

---

[1] - فالقرار 2170 الصادر بتاريخ 15 أوت 2014 بين القلق الدولي إزاء الاستخدامات السيئة للتكنولوجيا ، سيما فيما يتعلق بالتجنيد و التمويل . و القرار 2178 الصادر بتاريخ 24 سبتمبر 2014 بين أن الحظر المقيد للاستعمالات التقنية عليه أن يراعي الحقوق و الحريات الاساسية . و القرار 2199 الصادر بتاريخ 12 فيفري 2015 عبر عن القلق المتزايد للعنف الالكتروني . و أخيرا القرار 2253 الصادر بتاريخ 17 ديسمبر سنة 2015 المعادة الدولية لتنظيم القاعدة المرتكزة في نشاطاتها الارهابية على تكنولوجيا المعلومات . ماخوذة من ولد يوسف ميلود ، "الارهاب الالكتروني و الطرق الحديثة لتكوين التنظيمات الجهادية عبر شبكات الانترنت" ،مجلة الدراسات القانونية ، المجلد 3 ، العدد 2 ، ص 05 .

[2] - حيث قام هؤلاء الهاركز بانشاء برامج تحكم بلغة " أكتف أكس " مصمم للعمل عبر الانترنت ، حيث يقوم بتحويل الاموال من الحساب المصرفي للمستخدمين ، و أصبح بامكان هؤلاء الهكرة سرقة الاموال من أرصدة مستخدمي "كويكن" في جميع أنحاء العالم . المرجع نفسه ، ص 6

[3] - و تم ذلك باستخدام غاز السارين قامت به جماعة الحقيقة المطلقة المتطرفة ، حيث أدى إلى قتل 12 شخص و جرح 5 آلاف ، المرجع نفسه ، ص 7 .

[4] - و تم التخطيط للعملية عبر أدوات تكنولوجية الاتصال و المعلومات و الاستعانة ببرامج جوجل ايرث لتحديد الشوارع و التدريب و اجراء الاتصالات عبر الاقمار الصناعية و الاستعانة بالانترنت ، و خلال هذه العملية تمكن 10 افراد من السيطرة على المدينة في دقائق معدودة و ضرب فندق تاج محل و "أوبروي و نريمان هاوس " و هي العملية التي تبنتها منظمة عسكر طيبة المعادية للهند . انظر علي عبد صادق ، المرجع السابق ، ص 100.

1- تعريفه و يراد به اندماج المكونات الالكترونية بالمكونات البشرية [1]، و تجاوز هذا المفهوم الانترنت ليضم كل الاتصالات و الشبكات و قواعد البيانات و مصادر المعلومات . و اصبحت بنية النظام الالكتروني تعني المكان الذي لا يعد جزءا من العالم المادي أو الطبيعي ، فهي ذو طبيعة افتراضية رقية الكترونية .

و يتعامل الفضاء الالكتروني مع المعلومات حسب المصلحة المتوخاة و المبتغاة سواء كانت اقتصادية أو سياسية أو ايديولوجية ، فبينما تسيطر قلّة من الدول على القدرات التكنولوجية ، نجد المعلومة المتنقلة عبر هذه المساحة الافتراضية متاحة للجميع و التزامها يخص المعرفة بقواعد التشغيل .

وقد عرف النظام المعلوماتي في قانون الأونسترال النموذجي بالمادة 2 الفقرة 6 بشأن التجارة الالكترونية بأنها "النظام الذي يستخدم لإنشاء رسائل البيانات ،أو إرسالها ، أو استلامها أو تخزينها أو لتجهيزها على أي وجه آخر".

كما تم تعريف نظم المعلومات بمعاهدة بودابست الدولية [2] بأنها" كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة ، و التي يمكن بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للمعلومات ".و من خلال هذه الاتفاقية يتبين ان أساس الجريمة هو النظام المعلوماتي .

عرفتها كذلك منظمة التعاون الاقتصادي و التنمية بانها " تشمل الحاسبات الآلية ووسائل الاتصالات و شبكات المعلومات التي يمكن تخزينها و معالجتها و استرجاعها و نقلها بواسطة هذه الحاسبات ووسائل الاتصالات أو شبكات المعلومات بما في ذلك برامج الحاسبات الآلية و جميع القواعد اللازمة لتشغيل هذه الانظمة و المحافظة عليها "[3].

---

[1] - و يعد ويليام جيبسون أول من استخدم كلمة cyber مقترنة بكلمة space لتظهر في مصطلح الفضاء الالكتروني في كتابه الكلاسيكي عام 1984 ، و جاءت جهود " نيل ستيفيسون " سبتمبر عام 1989 لتحديد مفهوم شامل للفضاء الالكتروني بانه ذلك المحتوى و البديل الكوني الذي يمكن من خلاله للناس أن تشارك فيه .علي عبد صادق ، المرجع السابق ، ص 39 .

[2] - هي معاهدة دولية تضم العديد من الدول الاوروبية التي اجتمعت في بودابست بالمجر لوضع اتفاقية دولية لمكافحة الجريمة المعلوماتية في 23 نوفمبر 2001 http://conventions.coe.int/treaty/en/reports/html/185.htm

[3] - ايمن عبد الله فكري ، الجرائم المعلوماتية – دراسة مقارنة في التشريعات العربية و الاجنبية - ، الطبعة الاولى ، مكتبة القانون و الاقتصاد ، الرياض ، 2014 ، ص 25

و اصبح تبادل المعلومات عبر العالم الافتراضي لتحقيق مآرب عُنفية الشكل الجديد في ساحات الحروب الالكترونية بين الدول خصوصا[1] .

2- اثار استعمالات الفضاء الالكتروني : تغيرت الكثير من المعتقدات الدولية بعد أن تبين قصور الدولة سياديا على التحكم في أمنها ، سيما في تحويط البنية التحتية سواء المدنية منها أو العسكرية .فبعد الهجمات التي تعرضت لها أستونيا ومحاولات الاختراق في المانيا و فرنسا وبريطانيا و نيوزيلندا سنة 2007 ، اصبح المجتمع الدولي اكثر وعيا لمواجهة هذه الظاهرة الاجرامية[2] .

و ساهم النمو في مجتمع المعلومات في زيادة معضلة الامن حول ضمان سرية البيانات وارسالها و استقبالها و تخزينها و مدى تغييرها و تأمين الثقة فيها ، و كذا حماية نُظمها من الهجمات ذات الطابع التقني[3].

كما أن المرونة في تبادل المعلومات الكترونيا مَهَّد للتأثير على الرأي العام العالمي ، و سهّل جلب تعاطفه بغرض التعبئة و الحشد و الحصول على المساندة ، لتتوسع دائرة الفاعلين في الجرم الالكتروني و تكون مكسبا في عملية صنع السياسة الخارجية للدول . اصبح الفضاء الالكتروني كذلك سببا في حشد الاهتمام بقضايا دولية مثل الارهاب أو الفقر أو المرض أو الاحتباس الحراري و غيرها من القضايا ذات الطابع الانساني .السبب الذي هَبَّت لأجله الدراسات المختلفة،

[1] - و قد اقرت هيئة الاركان الامريكية تعريفا للفضاء الالكتروني من وجهة نظر عسكرية بانه :" مجال يتميز باستخدام الالكترونيات و الكهرومغناطيسية لتخزين تأثيرات متحركة أو ساكنة ضد الاشارات (الرادار – واجهزة الاتصال) و نقاط ربط و شبكات النظام الدفاعي ، حيث يتم الوصول إلى الهدف بسرعة الضوء أو بسرعة الصوت عند استعمال قدرتها الفضائية الالكترونية " و اعلنت القوات الجوية الامريكية في 7 ديسمبر 2005 تعريفا جديدا لمهامها القتالية بان حددت مهمة القوات الجوية في تسلم المهام للدفاع عن الو.م.ا و مصالحها العالمية بقدرتها على الطيران و القتال في الجو و الفضاء الخارجي و في الفضاء الالكتروني " . علي صادق ، المرجع السابق ، ص ص 42-43 .

[2] - في شهر ابريل و ماي ن سنة 2007 تم استخدام هجما الفضاء الالكتروني ضد المؤسسات الحكومية في الدول فتعرضت استونيا إلى هجمات استهدفت شل حركة بنياتها التحتية و ذلك إثر خلاف سياسي بين الاقلية الروسية و الحكومة . و في سبتمبر سنة 2007 اتهمت الصين بانها تقف وراء هجمات عبر اختراق أجهزة الكمبيوتر الخاصة بوزارة الدفاع الامريكية ، كما اتهمت بالمسؤولية عن هجمات مماثلة على المانيا و فرنسا و بريطانيا و نيوزيلندا، كما اعلنت الصين من جانبها انها تقع هي الاخرى ضحية هجمات . و شهدت الحرب الجورجية الروسية عام 2008 استخداما للفضاء الالكتروني في ضرب المواقع و الخدمات الحكومية في كلا البلدين . علي عبد الصادق ،المرجع السابق ، ص 19 .

[3] - محمد علي سكيكر ، المرجع السابق ، ص 10

شملت العلوم الاجتماعية و علم النفس و العلاقات الدولية و القانون الدولي و التعليم و الفلسفة و العلوم الاقتصادية [1].

ب/ دعائم جريمة الارهاب الالكتروني

للإرهاب الالكتروني مظهرين أحدهما مادي يتمثل في الحاق الضرر بالحق في الحياة وسلامة الجسم او الملكية الخاصة أو عامة ، و الآخر معنوي يتمثل في احداث الرعب لدى الناس و حمل دولة او منظمة دولية على القيام بعمل أو الامتناع عنه [2].

يتم استخدام الفضاء الالكتروني استخداما ارهابيا بصورة غير مباشرة عن طريق تسهيل عملية التنفيذ للعمل الارهابي بالاستناد الى الادوات التالية :

1- **استخدام العنف و التهديد به** :بحيث لا يهدف الارهابيون إلى القضاء على أرواح الضحايا و الاعتداء على ممتلكاتهم فحسب بل يحرصون على زرع الرهبة بين المجتمعات لتمرير اجندتهم .

2- **استخدام احدث وسائل الاتصالات** : لجمع و تبادل المعلومات عبر الشبكة المعلوماتية سيما عن المواقع الحيوية و بنيتها التحتية [3].

3- **اختراق المواقع الالكترونية** : تعريفا هو محاولة الدخول غير المشروع أو اساءة استخدام نظام أو شبكة الحواسب [4] ، من اجل تغيير محتوياته أو سرقة معلومات سرية أو تعطيل الموقع عن العمل أو الاستيلاء عليه بشكل كامل. و عادة ما يضع المهاجمون بعد نجاح مهمتهم رسائل في الموقع تعلن اختراقه . على ان عملية الاختراق تمر بمرحلة التسلل اولا على المواقع الرسمية للمؤسسات الحكومية أو الشخصية أو البريد الالكتروني ، ثم عملية الاغراق بالرسائل الالكترونية بإرسال عدد كبير بأحجام ضخمة غير مفيدة دفعة واحدة و في وقت متقارب قصد التأثير على السعة التخزينية للحواسيب الآلية المستهدفة ، فتتوقف عن العمل بسبب امتلاء منافذ الاتصال و كذا قوائم الانتظار لتنقطع الخدمة التي توفرها هذه الحواسيب .

---

[1] - بن يحي الطاهر ناعوس ، مكافحة الارهاب الالكتروني ضرورة بشرية و فرضية شرعية www.alukah.net

[2] - محمد عزيز شكري ، الارهاب الدولي ، طبعة أولى ، دار العلم للملايين ، بيروت ، 1991 ، ص 20 .

[3] - علي عدنان الفيل ، المرجع السابق ، ص 73

[4] - . معتز محيي عبد الحميد ، المرجع السابق ،ص 07

و من الاسباب التي يسّرت عملية الاختراق: ضعف الكلمات السرية و عدم وضع برامج كافية لحماية المواقع من الهجمات و عدم التحديث المستمر لهذه البرامج[1] ، و اخيرا استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر أو استخدام برامج و أنظمة غير موثوقة أمنيا [2]

4- **نشر الفيروسات الالكترونية** : هي عبارة عن خطة في شاكلة برامج مُخصّصة لترتيب الملفات المتداولة عبر الحاسبات الآلية ترتيبا يُغيّر من محتوياته إما بالإزالة أو التعديل او التخريب لأجل الحاق الضرر بالحاسوب أو السيطرة عليه [3].

5- **الحرب الاعلامية** : يراد بها توجيه الرأي العام العالمي لمقتضيات مختلفة عبر الفضاء الالكتروني باستعمال النص أو الصوت او الصورة ، لحشد المساندين و الحصول على التمويل لتمرير مخططاتهم و تنفيذها في الميدان [4].

6- **التدريب الارهابي الالكتروني** : يعد التدريب من اهم هواجس التنظيمات الارهابية و قد ساعدت الشبكة المعلوماتية بما تحتويه من خدمات مميزة على هذه المهمة ، بل أقدمت بعض الجماعات بإنتاج أدلة ارشادية للعمليات الارهابية تتضمن وسائل التدريب و التخطيط و التنفيذ و التخفي [5].

7- **التجسس الالكتروني** : هي عملية اقتناء أو نشر أو البحث عن أشياء مهما كانت صياغتها المادية أو القانونية أو معلومات سرية لهياكل حيوية أو البنيات التحتية ، سيما العسكرية أو الاقتصادية لمصلحة الافراد أو المنظمات أو الدول خصوصا المتصارعة تكنولوجيا [6].

---

[1] - بن مرزوق عنترة ، "جريمة الارهاب الالكتروني و آليات العلاج"، مجلة الحقوق و العلوم الانسانية ، المجلد 11 ، العدد 2 ، 2018 ، 515.

[2] - علي عدنان الفيل ، المرجع السابق ، ص 78

[3] - توفيق مجاهد و طاهر عباسة ، المرجع السابق ، ص 85

[4] - علي عبد صادق ، المرجع السابق ، ص 126. و أمير فرج يوسف ، المرجع السابق ، ص 134

[5] - غادة نصار ، المرجع السابق ، ص 29 .

[6] - ساري خالد ، الاتجاهات في أمن المعلومات و أمانها ، العبيكان للنشر و التوزيع، الرياض ، ص 211.
و بن عامر عوينات ،"الارهاب الالكتروني: المفهوم و الجهود الدولية و الاقليمية لمكافحته" ، مجلة الاستاذ الباحث للدراسات القانونية و السياسية ، العدد 6 ، المركز الجامعي تندوف ، 2017 ، ص 39

علاوة على كل ما سبق هناك ادوات اخرى يمكن ان تسهم في العمل الارهابي تمثل في اصدار البيانات الالكترونية و انشاء المواقع الارهابية الالكترونية ، و تدمير البيانات و النظم المعلوماتية .

البند الثالث : استقلالية عناصر جريمة الارهاب الالكتروني

يستقل عن الارهاب التقليدي بالآتي :

1- الارهاب الالكتروني لا يحتاج في ارتكابه الى العنف و القوة بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية و مزود ببعض البرامج اللازمة .

2- يتسم الارهاب الالكتروني بكونه جريمة ارهابية متعدية الحدود و عابرة للدول و القارات وغير خاضعة لنطاق اقليمي معين . و هي المسألة التي رتبت سلبيات تخص المسائل التالية :

- عدم الوصول إلى مفهوم عام موحد حول النشاط الذي يمكن الاتفاق على تجريمه
- تعقد المشكلات النظامية و الفنية الخاصة بتفتيش نظام معلوماتي خارج حدود الدولة أو ضبط معلومات مخزنة فيه أو الامر بتسليم المجرمين [1].

3- تنوع الفاعلين في استخدامات هجمات الارهاب الالكتروني بين:

- **الارهابيين المستخدمين للفضاء الالكتروني** في التجنيد و التعبئة و التخطيط و التنسيق و التمويل و جمع المعلومات . او في استخدام هجمات الفضاء الالكتروني كسلاح وهدف ضد أعدائها . و يمثل تنظيم القاعدة نموذجا لاستخدام الجماعات الارهابية و دون القومية للفضاء الالكتروني
- **الدول القومية** : تستخدم الدولة الفضاء الالكتروني كأداة للحرب ضد دولة اخرى معادية أو في مجال الاستخبارات أو أن تقوم الدول بالتعاون مع جماعات إرهابية أو أفراد للإضرار بدولة أخرى .
- **المتعاطفون مع الارهابيين** بفضل الاتصال و التواصل المدعم بأدوات الاقناع على مواقع التواصل الاجتماعي خصوصا تم حشد و تجنيد الافراد للمشاركة في الحركة الارهابية او على الاقل كسب مساندتهم ماديا

---

[1] - صليحة محمدي و شفيعة حداد ، "الارهاب الالكتروني و الامن القومي للدول : نمط جديد و تهديدات مختلفة" ، المجلة الجزائرية للامن و التنمية ، المجلد 8 ، العدد 15 ، 2019 ، ص 67

4-صعوبة اكتشاف جرائم الارهاب الالكتروني و نقص الخبرة لدى بعض الاجهزة الامنية والقضائية في التعامل مع مثل هذا النوع من الجرائم .و كذا صعوبة الاثبات لسرعة تغييب الدليل خاصتها. و ذلك للأسباب التالية :

- أنها جريمة لا تترك أثرا بعد ارتكابها .
- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- انها تحتاج خبرة فنية يصعب على المحقق التقليدي التعامل معها.
- أنها تعتمد على الخداع و التضليل في التعريف بمرتكبيها .
- ترتكب من قبل شخص ذو دراية فائقة بالانترنت.

5-**مرتكب جريمة الارهاب الالكتروني محترف** في الغالب من ذوي التخصص في مجال تقنية المعلومات أو اشخاص لهم قدر من المعرفة و الخبرة في التعامل مع الحاسوب و الشبكة المعلوماتية [1] .

البند الرابع : مكافحة الارهاب الالكتروني

التوحيد الدولي للتجريم الالكتروني اصبح ضرورة للتعاون ، و اولاها مبادرات الامم المتحدة، حيث عُقدت عدّة مؤتمرات على مستواها لتطويق جريمة الارهاب الإلكتروني امتدت لفترة زمنية معتبرة من سنة 1985 [2] الى سنة 2010 أو تلك التوصيات التي انتهت اليها كل من الجمعية الدولية لقانون العقوبات و بتأطير جاد من هيئة الامم المتحدة سنة 1994[3].

كذلك اجتماع هيئة الامم المتحدة في القاهرة سنة 1995 [4]، ركز على حماية الحريات الاساسية للأفراد المتعلق بالخصوصية و الملكية الفكرية و مخاطر تعرضها للخرق . و يكفي انه سنة 2000 تم التوقيع على اتفاقية مكافحة اساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية

---

[1] - علي عدنان الفيل ، المرجع السابق ، ص 112 .

[2] - يتعلق بمؤتمر ميلانو عام 1985 الذي كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية و الاعتداء على الحاسب الآلي و اعداد تقرير يعرضه على المؤتمر الثامن و الذي عقد فعلا سنة 1990 ليؤكد على اهمية الاستعمالات التكنولوجية في مواجهة هذه الظاهرة الاجرامية . سعيد عبيدي ، المرجع السابق ، ص 15

[3] - يتعلق الامر بمؤتمر الامم المتحدة الذي عقد في ري ودي جانيرو عام 1994 .المرجع نفسه ، ص 16 .

[4] يتعلق الامر بمؤتمر الامم المتحدة لمنع الجريمة و معاملة المجرمين في القاهرة عام 1995 . انظر صباح كزيز وآمال كزيز ، "الارهاب الالكتروني و انعكاساته على الامن الاجتماعي – دراسة تحليلية – "، مجلة التراث ، المجلد 8 ، العدد الاول ، 2018 ، ص 316 .

بإشراف الامم المتحدة التي أكدت في مادتها الاولى على أنه " ينبغي للدول أن تكفل عدم توفير قوانينها و ممارساتها ملاذا آمنا للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض اجرامية ."

التعاون الاوروبي له نظرة من خلال اتفاقية "بودابست" و هي متنفس دولي وضع القواعد الاجرائية لجرائم التقنية سيما القرصنة و ذلك بالتعاون مع كندا و اليابان و جنوب افريقيا والولايات المتحدة الامريكية حيث عرضت للتوقيع عليها سنة 2001 ، و دخلت حيز التنفيذ سنة 2004 .و بدورها دعت إلى إذابة الجهود الفردية في قالب تعاون دولي .

و لابد من الاشادة بدور المنظمة العالمية للملكية الفكرية ، حيث شكلت مجموعة عمل تضم عدد كبيرا من الخبراء بهدف دراسة الاساليب المناسبة لحماية برامج الحاسب الآلي من خلال اخضاعها لقوانين حماية حق المؤلف . و كذا الدور الفعال للاتحاد الدولي للاتصالات في اطلاق برنامجه سنة 2007 بوضع ورقة نموذجية هي خارطة طريق لمكافحة الجريمة المعلوماتية .

أما الشرطة الجنائية الدولية الانتربول فقد اسست عدة مراكز اتصالات اقليمية في كل من طوكيو ، نيوزيلندا ، نيروبي ، أذيجان ، بيوس أيرس من أجل تلقف الادلة . و تم التحضير سنة 2000 لمسودة حول الجريمة و الارهاب الالكتروني في جامعة ستاندفورد و أكدت من ان نجاح الاعمال العُنفية سببه الثغرات الامنية للاماكن المستهدفة .

كثفت الجهود الدولية بعد أحداث 11 سبتمبر 2001 لتأخذ شكل تحرشات من الولايات المتحدة الامريكية في اقلاق أمن الدول بحجة مكافحة الارهاب ، ففي سنة 2007 أعلن سلاح الجو الامريكي تشكيل قيادة في العالم الالكتروني بوضع منظومة متكاملة لتدريب و تجهيز قوات ضمن سلاح الجو . ليتم الرد عليه من قبل الاتحاد الدولي للاتصالات بإطلاق مبادرته الاستراتيجية للأمن الالكتروني عام 2007 ضد اخطار الفضاء الالكتروني و العمل على تعزيز أمن البنية التحتية الكونية للمعلومات.[1]

و نرصد موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 بأن حثت الدول الأطراف بتنظم قوانيها الداخلية في تجريم هذه الافعال ، و استتبعتها بجملة من التدابير الاحترازية و تكثيف الجهود فيما بينها لصد الاختراق المعلوماتي غير المشروع ، و البداية بتقديم قائمة للأفعال التي تشكل الركن المادي لجريمة الارهاب الالكتروني بأن عددت المادة 15 منها جملة تمثلت أساسا في نشر أفكار التطرف و طرق صناعة المتفجرات و الفتن و الاعتداء على الديانات و المعتقدات . كما اقدمت الاتفاقية على تقديم تعريف للمواقع الالكترونية بأنها " تلك

[1] - علي عبد الصادق ، المرجع السابق ، ص 18 .

المواقع التي تنتج المعلومة على شبكة الانترنت و تساعد على نشر و تداول الافكار الضالة ، والتحريض على استخدام العنف من أجل تحقيق أهداف خاصة بالقائمين عليها تحت مظلات ومسميات دينية و سياسية ، بهدف إلحاق أكبر ضرر بالآخرين دولا و شعوبا ".

التشريع الجزائري في مواجهة جرائم المعلوماتية في الفضاء الافتراضي

عدّد المشرع الجزائري النصوص الممثلة للجرائم المعلوماتية و على رأسها قانون العقوبات المعدل سنة 2004 [1]، فجرّمت الافعال المسيئة لاستعمالات التقنية بإحداث قسم جديد في قانون العقوبات بعنوان " المساس بأنظمة المعالجة الآلية للمعطيات ". و يتعلق الامر بتلك الافعال المنصوص عليها بالمادة 394 مكرّر و التي تدور جميعها حول عملية الاختراق للنظام المعلوماتي من الدخول خلسة إلى البقاء غير المشروع و تعديل أو حذف معطيات المنظومة المعلوماتية أو الاضرار بنظام تشغيلها .

أو ما تعلق بإدخال أو تعديل أو إزالة معطيات خلسة في هذه المنظومة المعلوماتية [2]، او التخطيط عمدا بتصميم أو بحث أو توفير أو نشر معطيات تُمكّن من ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات . أو متى ارتكبت هذه الافعال مساسا باستقرار الامن أو بالبنية التحيتية [3] .

و تدخل قانون الاجراءات الجزائية في تعديله سنة 2004 [4]لتبيان الجزاءات و المتابعة والتحقيق . و البادرة الطيبة كانت من خلال احداث المحاكم الجزائية ذات الاختصاص الموسع للنظر في الجرائم الماسة بعالم التقنية [5].

و وسعت صلاحيات ضباط الشرطة القضائية بتمديد اختصاصها الاقليمي لتحقيق في هذه الجرائم بقواعد استثنائية تخص تفتيش المحلات السكنية دون الالتزام بالركن الزمني بشرط الحصول على إذن من وكيل الجمهورية المختص ، و أجاز المشرع هذه العملية دون حضور المشتبه فيه و دون شهود . مع مراعاة السر المهني عند إجراء التفتيش .

---

[1] - القانون. العقوبات 04-15 المؤرخ في 10 نوفبر سنة 2004 ، ج ر 71 . المعدل و المتمم للامر 66-156 المؤرخ في 08 يونيو سنة 1966 ، الذي يتضمن قانون قانون العقوبات

[2] - المادة 394 مكرر 1 من قانون العقوبات

[3] - انظر المادتين 394 مكرر 2 و 394 مكرر 3

[4] - القانون 04-14 مؤرخ في 10 نوفبر 2004 المعدل لقانون الاجراءات الجزائية ، ج ر 71 المعدل و المتمم للامر 66-155 المؤرخ في 08 يونيو سنة 1966 الذي يتضمن قانون الاجراءات الجزائية .

[5] - انظر المواد 37 و 40 و 329 من قانون الاجراءات الجزائية

تحقيقا لفعالية أكثر بغرض جمع الادلة يجوز استعمال أساليب خاصة للتحقيق منها اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية ، و التقاط و بث و تسجيل الكلام أو التسرب من خلال تسخير ضباط الشرطة أو اعوانهم او اشخاص معينين لخدمة مهمة ايقاف مرتكبي هذه الجرائم [1].

الخاتمة

جريمة الارهاب الالكتروني و غيرها من المستجدات في العالم الافتراضي هو الخطر المستقبلي ، المتمثل في حرب تكنولوجية بين المالكين و المسيطرين على التقنية و المعلوماتية المتطورة .

و لان الفاعل في جريمة الارهاب الالكتروني أصبح الغازي الجديد نجده غير مرتبط بالضرورة بفكرة المواطنة ، فقد تكون الاسباب مدفوعة بدواعي نفسية كالانتقام أو ايديولوجية أو دينية .

و تكمن خطورة هذا النوع من الجرائم في انها لا تعرف الحدود الزمانية او المكانية ، و لا ترتبط بأدلة مادية تدل عليها أو على من يرتكبها .

و للحيلولة دون تنامي هذه الظواهر الاجرامية وجب للدول ان تكثف جهودها في تدويل القوانين المجرمة لهذه الافعال ، على ان تؤسس بشرعية و ليس لخدمة أهدافها التوسعية .

و يكون للمجتمع المدني دور مهم في منع و مكافحة الارهاب و خاصة الاسرة ، باعتبارها الموجه الاول للاجيال الناشئة ، و العمل على بعث القيم الصحيحة بالتعاون مع التكتلات الجمعوية و الاهلية بصفة عامة الناشطة اجتماعيا و دينيا .

و الاهتمام بالدراسات الاكاديمية أصبح بشكل أكثر من ضرورة داخل الوسط الجامعي على وجه الخصوص بوضع هذه الجرائم تحت المجهر النظري و العملي من خلال إلقاء المحاضرات و الندوات العلمية .

[1] - المادة 65 مكرر 11 من قانون الاجراءات الجزائية

ير المحررات الإدارية الالكترونية

Forging electronic administrative documents.

أ. قارة تركي الهام أستاذ مساعد قسم أ

معهد الحقوق والعلوم السياسية

المركز الجامعي مغنية - الجزائر

مقدمة:

بظهور عصر التكنولوجيا ظهر ما يسمى بالإدارة الالكترونية، حيث أن الإدارة أصبحت تتخلى تدريجيا على المعاملات الورقية ليحل محلها الاستخدام الواسع لتكنولوجية المعلومات[1]. فلقد أصبح تبادل المعلومات وتقديم الخدمات من قبل الإدارة للأفراد يتم بسرعة عالية وتكلفة منخفضة بواسطة الحاسوب والانترنيت[2]، ليظهر بذلك نوع جديد من الوثائق الإدارية تسمي بالوثائق الإدارية الالكترونية.

ولقد أعطى المشرع الجزائري للمحررات المكتوبة بالشكل الالكتروني نفس حجية المحررات الورقية طبقا للمادة 323 مكرر من القانون المدني[3]، شريطة إمكانية إثبات هوية محررها بأن يكون توقيعه بأرقام سرية تميزه عن غيره من الموظفين، مع إمكانية حفظ هذه الوثائق وذلك حسب ما جاء في المادة 9من المرسوم التنفيذي 15_04[4] .

على انه إضافة إلى ضرورة صحة التوقيع الالكتروني باعتباره بيانا ضروريا لازما لصحة الوثيقة الإدارية الالكترونية، لابد أن تتضمن هذه الأخيرة جميع البيانات الضرورية التي تتضمنها الوثيقة الإدارية الورقية لإضفاء الطابع الرسمي عليها وهي: الرأسية، الطابع، الرقم التسلسلي، التاريخ ومكان تاريخ الوثيقة الإدارية، المرسل والمرسل إليه، العنوان والموضوع.

---

[1]- السالمي علاء عبد الرزاق محمد، الإدارة الالكترونية ، دار وائل للنشر، عمان ، الأردن، 2007، ص.ص.2_3.

[2]-حسين محمد الحسن، الإدارة الالكترونية، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، 2010، ص.32.

[3]-الأمر رقم 75_58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، المعدل والمتمم بالآمر رقم 05_10 المؤرخ في 20 جوان 2005، ج،ر، ج،ج، ع44 الصادرة في 26 جوان2005.

[4]-القانون رقم15_04 المؤرخ في 15 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر، ج.ج،ع.6، الصادرة في 10 فبراير 2015.

إلا أن هذه المحررات الإدارية سواء كانت ورقية أو الكترونية قد تكون عرضة للتغير عما هي عنه في الحقيقة[1]، تحت ما يسمى بفعل التزوير.

وبناء على ما تقدم تثار إشكالية ما هو موقف المشرع الجزائري من مسألة تزوير المحررات الإدارية الالكترونية؟، أو بمعنى آخر ما هي الأفعال التي تعتبر من قبيل التغيير لحقيقة مضمون المحرر الإداري الالكتروني؟

للإجابة على هذه التساؤلات سنعتمد على المنهج الاستدلالي والمنهج التحليلي لنصوص القانونية المتعلقة بهذا المجال، وفق خطة ثنائية نتناول فيها:

أولا: تزوير المحررات الإدارية الالكترونية وفق قانون العقوبات

ثانيا: تزوير المحررات الإدارية الالكترونية وفق قانون رقم 15_04

أولا: تزوير المحررات الإدارية الالكترونية وفق قانون العقوبات

حتى يحوز المحرر الإداري الورقي الرسمية يجب أن يصدر من موظف عام مع مراعاة الشروط الشكلية التي تتطلبها النصوص المنظمة لها[2].

ومادام إن المشرع الجزائري قد قام بالمساواة بين المحرر الورقي والمحرر الالكتروني في الحجية[3]، فان نفس الشروط السالف ذكرها يجب أن تتوافر لإضفاء الرسمية على الوثيقة الإدارية الالكترونية.

وكما سبق الإشارة إليه أن هذه المحررات قد تكون عرضة للتزوير إما من قبل موظف(أ) أو من قبل شخص لا تتوافر فيه هذه الصفة (ب) وهذا ما تناوله المشرع العقابي الجزائري، علما انه تحدث عن ذلك دون أن يميز بين ما إذا كانت هذه المحررات العمومية ورقية أو الكترونية، فعلى أساس ذلك يتم تطبيق نفس الأحكام في الحالتين.

أ)التزوير الواقع على المحررات الإدارية الالكترونية من قبل موظف:

يكون الموظف العام أو القائم بخدمة عامة مسؤولا عن المحررات الإدارية سواء ورقية أو الكترونية، كونه ملزم بالسهر على حماية الوثائق الادارية وعلى أمنها[4]. والموظف قد يكون طرفا في الوثيقة الإدارية كمحرر لها وقد لا يكون طرفا فيها، بمعنى أن تزوير هذه الوثيقة الإدارية قد يكون من

---

[1]-الأحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، دار هومه، الجزائر، 2004، ص.239.

[2]-صفاء فتوح جمعة، مسؤولية الموظف العام في إطار تطبيق نظام الإدارة الالكترونية، دار الفكر والقانون، المنصورة، مصر، 2014،ص.108.

[3]-المادة324 مكرر قانون مدني، المصدر السابق.

[4]-صفاء فتوح، المرجع السابق، ص.112، بالإضافة إلى المادة 49 من الأمر رقم06_03 المؤرخ في 15 يوليو2006، يتضمن القانون الأساسي العام للوظيفة العمومية،ج.ر،ج.ج،ع.46، الصادرة في 16 يوليو2006.

قبل الموظف الذي قام بتحريرها ، وقد يكون من غير محررها أي موظف لا علاقة له بالوثيقة الإدارية لا كمحرر ولا كمحرر إليه.

)المزور هو موظف محرر الوثيقة الإدارية:

لقد جاء في نص المادتين 214 و215 من قانون العقوبات، على أنه كل قاض أو موظف أو قائم بوظيفة عمومية قام بارتكاب أثناء تأدية وظيفته إحدى الأفعال الواردة في نص هتين المادتين فانه يكون مسؤولا عن جريمة التزوير.

أي أن المشرع العقابي قد حصر الأفعال التي تعتبر تزويرا للمحررات الإدارية الرسمية والالكترونية على حد السواء، وهي:

- ✓ وضع توقيعات مزورة.
- ✓ إحداث تغيير في المحررات أو الخطوط أو التوقيعات.
- ✓ انتحال شخصية الغير والحلول محلها.
- ✓ الكتابة في المحررات العمومية أو التغيير فيها بعد إتمامها أو قفلها.
- ✓ تزوير جوهر الوثيقة الإدارية أو ظروفها بطريق الغش، على أن يكون ذلك:
  - ➢ اما بكتابة اتفاقات خلاف تلك التي دونت أو أمليت من الأطراف.
  - ➢ أو بتقرير الموظف لوقائع يعلم أنها كاذبة في صورة وقائع صحيحة .
  - ➢ أو بالشهادة كذبا بان وقائع قد اعترف بها أو وقعت في حضوره.
  - ➢ أو بإسقاطه عمدا الإقرارات التي تلقاها.
  - ➢ أو بتغييره عمدا الإقرارات التي تلقاها.

فعلى أساس ذلك، حتى تقوم المسؤولية الجزائية للموظف هنا لابد من توافر ثلاثة شروط وهي:

- ✓ شرط الصفة: أي أ يكون المزور موظف له علاقة بالوثيقة الإدارية.
- ✓ شرط الزمن: أي أن يقع فعل التزوير أثناء تأدية الوظيفة.
- ✓ شرط الفعل: بحيث انه لا يعتبر تغييرا للحقيقة إلا الأفعال السالف ذكرها، وهي الواردة في المادتين214 و215 من قانون العقوبات.

فمتى اجتمعت تلك الشروط الثلاثة، فا الفاعل يعاقب بالسجن المؤبد.

على انه اذا تم استعمال تلك الوثيقة المزورة، فانه يعاقب الفاعل الذي يعلم بأنها مزورة بالسجن من 5 سنوات الى 10 سنوات طبقا للمادة218 من قانون العقوبات.

2)مسؤولية الموظف عن الافعال المرتبطة بفعل التزوير

يتعلق الأمر هنا بحالة استعمال الوثيقة المزورة، بالإضافة إلى حالة الإدلاء بتقرير مزور.
بحيث أنه إذا تم استعمال الوثيقة الإدارية الالكترونية المزورة، فانه يعاقب الفاعل الذي يعلم بأنها مزورة بالسجن من 5 سنوات إلى 10 سنوات طبقا للمادة218 من قانون العقوبات.
كما أنه يعاقب الموظف الذي ليس طرفا في المحرر ويقوم بالإدلاء أمام موظف عام بتقرير يعلم أنه غير مطابق للحقيقة، بالحبس من سنة الى خمس سنوات وبغرامة من 500 الى 1000 دينار، طبقا للمادة 217 قانون عقوبات.

ب)التزوير الواقع على المحررات الإدارية الالكترونية من غير موظف:

كل شخص لا تتوافر فيه صفة موظف كقاضي أو موظف عام أو مكلف بخدمة عمومية، ارتكب أحد الأفعال المنصوص عليها في المادة216 قانون العقوبات من أجل تزوير المحررات الإدارية الرسمية بما فيها الالكترونية، سواء كان مخاطبا بهذه الأخيرة(أي المرسل إليه) أو غير مخاطب بها (أي ليس طرفا في الوثيقة الإدارية محل التزوير)، فانه يعاقب بالسجن المؤقت من 10 سنوات إلى 20 سنة وبغرامة من 1.000.000دج الى 2.000.000دج طبقا لنفس المادة السالف ذكرها.
على أن الأفعال المعتبرة تزويرا للمحرر الإداري الالكتروني قد حددها المشرع العقابي على سبيل الحصر وهي:

- ✓ التقليد أو تزييف الكتابة أو التوقيع.
- ✓ اصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هذه المحررات فيما بعد.
- ✓ إضافة أو إسقاط أو تزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها أو لإثباتها.
- ✓ انتحال شخصية الغير أو الحلول محلها.

كما أن كل من استعمل محررا إداريا يعلم بأنه مزورا، يعاقب فاعل ذلك بالسجن من 5 سنوات الى 10 سنوات طبقا للمادة 218 قانون العقوبات.

أما الإدلاء بتقرير مزور أمام موظف عام من قبل شخص غير طرف في الوثيقة الإدارية الالكترونية، مع علم هذا الأخير بعدم مطابقة المحرر للحقيقة، فانه يعاقب بالحبس من سنة إلى خمس سنوات و بغرامة من 500 دج إلى 1.00 دج وهذا ما جاء في نص المادة 217 من نفس القانون.

ثانيا: تزوير المحررات الإدارية الالكترونية وفق قانون 15_04:

لقد تناول القانون رقم 15-04 بيانا ضروريا واحدا يخص المحررات الإدارية الالكترونية والذي يتعلق بالتوقيع الالكتروني.

فإذا كان تزوير التوقيع اليدوي يقصد به تقليد التوقيع بطريقة تشبه التوقيع الأصلي، فان تزوير التوقيع الالكتروني هو أن يتم اعتماد التوقيع نفسه عن طريق الحصول عليه بطرق مختلفة، فالتوقيع الالكتروني المزور مطابق تماما للتوقيع الأصلي[1].

وما يلاحظ في هذا القانون هو أن المشرع الجزائري وان كان قد أعطى للتوقيع الالكتروني فعاليته القانونية وحجية قانونية كاملة أمام القضاء طبقا لنص المادة 9، بالإضافة إلى نصوص خاصة تنظم التعامل به وكذلك نصوص تجريمية مرتبطة باستعماله، إلا أنه أغفل مسألة التزوير الحاصل على التوقيع الالكتروني، هذا ما يثير التساؤل حول مدى امكانية تطبيق الأحكام العامة الخاصة بالتزوير الواردة في قانون العقوبات على التزوير الذي يمس المحررات الالكترونية.

إن الإجابة على هذه الإشكالية نجدها في نص المادة10 من اتفاقية العربية لمكافحة جرائم تقنية المعلومات21 ديسمبر2010 ، حيث عرفت جريمة التزوير ألمعلوماتي على أنها :" استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر وبنية استعمالها كبيانات صحيحة"، وما دام أن الجزائر قد صادقت عليها بموجب المرسوم الرئاسي رقم14-252 المؤرخة في 8 سبتمبر 2014[2]، فان الأفعال التي تشكل جريمة تزوير معلوماتي تدخل في إطار التجريم على المستوى الداخلي وبالتالي تطبيق أحكام قانون العقوبات عليها.

بالاضافة الى ذلك نجد أن المشرع العقابي في قانون العقوبات عندما تحدث عن تزوير المحررات الادارية لم يميز بين ما اذا كانت هذه المحررات ورقية أو الكترونية، لذلك تطبق احكام ذلك القانون على الحالتين.

الخاتمة:

إن هذه الدراسة الموجزة لموضوع تزوير المحررات الإدارية الالكترونية، أدى إلى الخروج بمجموعة من الاستنتاجات منها:

---

[1]- حفصي عباس، جرائم التزوير الالكترونية، دراسة مقارنه، أطروحة الدكتوراه في العلوم الإسلامية، كلية العلوم الإسلامية، جامعة أحمد بن بله، وهران، 2014-2015، ص.28-ص،96.

[2]-المرسوم الرئاسي رقم14_252 المؤرخ في 13 ذي القعدة1435 الموافق ل8 سبتمبر2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج.ر،ج.ج، ع.57ن الصادرة في 28 سبتمبر 2014.

✓ من حيث تعريف تزوير المحررات الإدارية الالكترونية:

- لاحظنا غياب تعريف للمشرع الجزائري له ومع ذلك هناك تعريف لتزوير التوقيع الالكتروني في الاتفاقية العربية لمكافحة جرام تقنية المعلومات.
- التعريف الذي يمكن أن نعطيه لتزوير المحررات الإدارية الالكترونية : كل تغيير يقع على الوثيقة الإدارية الالكترونية بواسطة وسائل تقنية المعلومات، مما يجعلها مغايرة لما هي عليه في الحقيقة وذلك من أجل استعمالها.

✓ إذا كان المشرع قد أحسن عندما وضع تنظيم خاص بمسألة التوقيع الالكتروني إلا أن ذلك غير كاف خاصة وأنه قد أغفل في الأحكام العقابية مسألة التزوير الذي قد يكون هذا التوقيع عرضة له.

✓ خضوع جرائم التزوير الواقعة على المحررات الإدارية الالكترونية إلى الإحكام العامة الواردة في قانون العقوبات، إلا أن ذلك يكون صعبا بالنسبة لتزوير التوقيع الالكتروني ما دام أن الأمر لا يتعلق بالتحقيق في التقليد وإنما استعمال نفس التوقيع بعد الحصول عليه بطرق مختلفة وهذه الأخيرة يصعب الكشف عنها.

فعلى أساس ذلك نطرح بعض التوصيات:

✓ وضع تنظيم عقابي مشدد يخضع له مرتكبي أفعال التزوير التي تقع على المحررات الإدارية الالكترونية، خاصة وان هدف هذه الأخيرة المصلحة العامة.

✓ إنشاء جهة مختصة في تقنية المعلومات تعمل على مستوى القضاء، من أجل البحث والتحري في الجرائم التي تقع على المحررات الادارية الالكترونية بما فيها جرائم التزوير.

الاستغلال الجنسي للقصر عبر شبكة الانترنت –البعد الوقائي والردعي في التشريع الجزائري-

Sexual exploitation of minors via the Internet - a preventive and deterrent dimension in Algerian legislation

د.**الحاج علي بدر الدين** أستاذ محاضر قسم أ
معهد الحقوق والعلوم السياسية
المركز الجامعي مغنية - الجزائر

بوعكاز خليل طالب دكتوراه
معهد الحقوق والعلوم السياسية
المركز الجامعي مغنية- الجزائر

مقدمة

لا ينكر أحد المنافع الكبيرة التي أفرزتها تكنولوجيا المعلومات وشبكات الأنترنت لما أحدثته من نقلة نوعية في حياة البشرية في مختلف أنماط التبادل المعلوماتي وكذا التعاقد الالكتروني وحتى في مجال الاستثمار، بل قد حولت العالم إلى قرية صغيرة وسهلت اتصال الناس ببعضهم البعض رغم البعد المكاني والاختلاف الزماني[1].

لكن وبالرغم من المنافع الكبيرة السابقة التي أفرزتها شبكات المعلومات العالمية فإنها أوجدت في المقابل مجالا خصبا لمجموعة من الجرائم الأخلاقية والمالية. بل وحتى الدول اليوم أصبحت تتسارع إلى حماية أمنها القومي عن طريق حماية أسرارها الالكترونية من أي اعتداء خارجي أو حتى داخلي خاصة في ظل تزايد عمليات قرصنة المنشآت الاقتصادية والتجارية علاوة على انتشار شبكات الارهاب السرياني التي توفر ملاذا للتنسيق بين مختلف التنظيمات الارهابية المتطرفة.

[1]- مازال هذا الاتجاه العام في استخدام الأنترنت في تزايد مستمر،فوفقا للتقديرات ستساوي حركة الانترنت العالمية سنة 2020 ما يعادل 95 ضعف إجمالي حركة الإنترنت العالمية سنة 2005، وسيكون عدد الأجهزة المتصلة بشبكات IP ثلاثة أضعاف سكان العالم عام 2020. أنظر، مؤشر شبكة سيسكو المرئية
https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
تاريخ الولوج للموقع 2020/04/03 على الساعة 15:28.

والاطفال[1] لم يسلموا هم الآخرون من هذه الثنائية المتضادة (سلبي -إيجابي) في التعامل بالأنترنت، حيث لا يمكن عزلهم عن هذه القرية الصغيرة فكثيرا ما يستعلمون الأنترنت في بحوثهم المدرسية أو بغرض قضاء وقت في الألعاب الإلكترونية[2] أو حتى في وسائل التواصل الاجتماعي وذلك كمتنفس لهم للتخلص من أية ضغوط أو حالات قلق أو اكتئاب، بل منهم من اعتبرها طريقة ملائمة لحل مشاكله الاجتماعية على المدى القريب.

هذا الاستعمال اليومي جعل الطفل في عرضة دائمة لنوع جديد من الاستغلال والذي بات يعرف قانونيا بالاستغلال الجنسي عبر الأنترنت حيث صارت تمثل موردا من موارد الحياة الاقتصادية للكثيرين من الأفراد غير الأسوياء الذين يتصيدون الأطفال لإشباع انحرافاتهم الجنسية بكل سرية[3]، بل إن الكثير من البلدان تعتمد في اقتصادها على تلك التجارة المربحة[4].

ففي بداية عام 2013 كانت قاعدة البيانات الدولية لصور الاستغلال الجنسي للأطفال التي تديرها الأنتربول قد مكنت من التعرف على 3000 ضحية و 1500 مجرم موزعين على 40

---

[1]- تعرف لنا المادة 02 من القانون رقم 12/15 المؤرخ في 15 يوليو 2015 المتعلق بحماية الطفل على أنه " كل شخص لم يبلغ 18 سنة كاملة. " الجريدة الرسمية عدد 39 لسنة 2015.

[2]- كلنا يتذكر لعبة الحوت الأزرق التي حصدت أرواح 08 أطفال ماتوا شنقا استجابة لأوامر اللعبة في حوادث متفرقة هزت مشاعر الجزائريين و جعلت السلطات الجزائرية في حالة استنفار قصوى أين أطلقت العديد من حملات التوعية الإعلامية في المدارس والمساجد والإعلام دعت فيها إلى توخي الحذر ومراقبة أكثر لاستخدام الأطفال للأنترنت.

[3]- أشارت دراسة الأمين العام للأمم المتحدة في عام 2006 بشان العنف ضد الأطفال إلى ما ذكرته منظمة الصحة العالمية من تعرض 150 مليون من البنات و 73 مليون من الأولاد دون 18 سنة لجماع جنسي قسري أو لأشكال العنف الجنسي والاستغلال التي تضمنت اتصالا جسديا. أنظر، تقرير صادر عن اليونيسيف حول الاستغلال الجنسي للأطفال في مختلف أنحاء العالم منشور في الموقع :

https://www.unicef.org/arabic/protection/files/World_Congress_Background_Ar.pdfت اريخ الولوج للموقع : 2020/04/03 على الساعة 22:56.

[4]- خالد مصطفى فهمي، حقوق الطفل ومعاملته الجنائية في ضوء الاتفاقيات الدولية –دراسة مقارنة- دار الجامعة الجديدة، الإسكندرية، 2007، ص.78.

بلد، إضافة إلى العثور على بيانات بشأن عدد كبير من الضحايا غير محددة هويتهم الذين لم يبدأ التحقيق في حالاتهم بعد.[1]

كما تشير دراسة حديثة قامت بها مؤسسة ICDL ARABIA سنة 2015 حول سلوك النشء والشباب العربي على الإنترنت والمخاطر التي يتعرضون لها على عينة مكونة من 404 مراهق تبلغ أعمارهم بين 14 إلى 18 عام، خلال الفترة ما بين 13 يوليو إلى 28 أغسطس 2014، بهدف التعرف على تجاربهم الشخصية عند استخدام شبكة الإنترنت، وأكدت أهم النتائج المتعلقة بالاستغلال عبر الإنترنت على أن نحو 48% منهم يقضون معظم أوقاتهم على الإنترنت في غرفهم دون إشراف البالغين، وأن نحو 16% تلقوا طلبات على الإنترنت بشأن

---

[1]- تقرير المقررة الخاصة الأستاذة نجاة معلا مجيد المعنية ببيع الأطفال واستغلالهم في البغاء وفي المواد الإباحية إلى مجلس حقوق الإنسان في دورته 25 بتاريخ 23 /2013/12 ص.06 منشور على الموقع- https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=52f8a8e64 تاريخ الولوج للموقع 2020/04/03 على الساعة 19:36.

وبعد دراسة مجموعة عشوائية من مقاطع الفيديو والصور المسجلة في قاعدة البيانات الدولية لصور الاستغلال الجنسي للأطفال، أصدر الإنتربول بالتعاون مع شبكة ECPAT ، تقريرا مشتركا في شباط/فبراير 2018 بعنوان "Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material." (نحو مؤشر عالمي للضحايا المجهولي الهوية في مواد الاعتداء الجنسي على الأطفال.وحددت الدراسة عددا من الاتجاهات المثيرة للقلق:

كلما كانت الضحية أصغر سنا، اشتدت الإساءة إليها.

تضمّن 84 في المائة من الصور ممارسة جنسية واضحة.

كان أكثر من 60 في المائة من الضحايا المجهولي الهوية من اليافعين دون سن البلوغ، ومن بينهم رضَّع وأطفال صغار.

كان 65 في المائة من الضحايا المجهولي الهوية من الفتيات.

من المحتمل أن تكون أشد صور الاعتداءات قسوة صورا لصِبية.

92في المائة من المجرمين الذين ظهرت صورهم كانوا من الرجال.

https://www.interpol.int/ar/2/10/1 تاريخ الولوج للموقع: 2020/04/03 على الساعة 23:09.

الحصول على معلومات شخصية من غرباء، كما تلقت نسبة مساوية (16%) أيضاً محتويات إلكترونية غير لائقة تضمنت روابط مواقع إلكترونية أو صور أو مقاطع فيديو وما إلى ذلك[1].

والجزائر ليست في مأمن من هذه الآفة الخطيرة التي تهدد أمن وأخلاق ومستقبل فلذات أكبادنا، الأمر الذي جعلها على حتمية مواجهتها بالطرق الردعية والوقائية . وبالتالي تظهر اهمية هذه الدراسة في الوقوف على اشكالية مدى الكفاية القانونية التي اعتمدتها الدولة في مواجهة هذه الظاهرة؟.

وعليه، سنحاول من خلال هذا البحث التعرض إلى مدى مواءمة التشريع الجزائي الجزائري مع الاتفاقيات الدولية الخاصة بمكافحة الاستغلال الجنسي للأطفال عبر الأنترنت (أولا) ثم نستعرض تقييم التجربة الجزائرية في مكافحة هذه الجريمة (ثانيا).

أولا: مدى مواءمة التشريع الجزائي الجزائري مع النصوص الدولية الخاصة بمكافحة الاستغلال الجنسي للأطفال عبر الأنترنت

كثيرة هي النصوص الدولية التي عنيت بحماية الأطفال أخلاقيا[2]، لكن ما يهمنا في هذه الدراسة هي تلك المتعلقة بحماية الأطفال من الاستغلال الجنسي عبر الأنترنت والتي تبنتها الجزائر،

---

[1]- تقرير السلامة على الأنترنت –دراسة بحثية حول سلوك النشء العربي على الأنترنت والمخاطر التي يتعرضون لها منشور على الموقعfile:///c:/users/n'tic/downloads/reports-cyber_safety-2015fتاريخ الولوج للموقع 2020/04/03على الساعة 15:50.

[2]- نذكر منها على سبيل المثال

اتفاقية الأمم المتحدة لحظر الاتجار بالأشخاص واستغلال دعارة الغير اعتمدت وعرضت للتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة المؤرخ في 1949/12/02 وبدأت في النفاذ 25يوليه 1951 حيث نصت المادة 17 على أن تتخذ الدول الأطراف تدابير لمكافحة الاتجار بالأشخاص من الجنسين لأغراض الدعارة (منشورة على الموقع http://hrlibrary.umn.edu/arab/b033.html) تاريخ الولوج للموقع 2020/04/04 على الساعة 08:15 .

الميثاق الأفريقي لحقوق الطفل ورفاهيته المنعقد في أديس أبابا جويلية 1990 ودخل حيز التنفيذ في 02 نوفمبر 1999 (صادقت عليه الجزائر بموجب المرسوم الرئاسي رقم 242/03 المؤرخ في 08 جويلية 2003 الجريدة الرسمية عدد41) والذي نص من خلال المواد 46-47 على حق الطفل في وقايته من سوء المعاملة والحماية من الاستغلال الجنسي ؛

مؤتمر ستوكهولم لمناهضة الاستغلال الجنسي التجاري للأطفال 1996 والذي جاء كامتداد للحملة الدولية للحد من دعارة الأطفال المرتبطة بالسياحة في آسيا؛
النظام الأساسي للمحكمة الجنائية الدولية الصادر في 17جويلية 1998والذي اعتبر في المادة 7 منه الفقرة 2 ان الاتجار بالأطفالواستغلالهم جنسيا يعد جريمة في حق الانسانية ؛
المؤتمر الدولي لمكافحة الاستغلال الجنسي للأطفال المنعقد في فيينا 1999 والذي أكد على ضرورة تدعيم التعاون الدولي في مكافحة الاستغلال الجنسي للأطفال على الأنترنت؛
الاتفاقية الأوربية بشأن الاجرام المعلوماتي بودابست 2001/11/23، (أنظر الموقع :
https://rm.coe.int/budapest-convention-in-arabic/1680739173والتي تعد أول بادرة دولية لمناهضة جرائم الاستغلال الجنسي للأطفال وحتى وإن كانت أوربية المنشأ فهي ذات نزعة دولية، إذ فتحت الباب أمام الدول الأخرى غير الأوربية من أجل الانضمام والمصادقة عليها، حيث نصت المادة 09 من هذه الاتفاقية على الجرائم المتصلة بالمواد الإباحية للأطفال وسعت إلى تدعيم الإجراءات التي تحمي الأطفال من الاستغلال الجنسي من خلال تحديث قانون العقوبات وجعله أكثر فعالية؛
المؤتمر العالمي الثاني لمناهضة الاستغلال الجنسي التجاري للأطفال والذي عقد في اليابان (يوكوهاما) في الفترة الممتدة من 18-20ديسمبر 2001 والذي جاء من أجل تنفيذ خطة العمل المعتمدة في المؤتمر الأول الذي عقد في ستوكهولم وتحديد المجالات الرئيسية للمشاكل او الثغرات التي تعوق من مكافحة أشكال الاستغلال الجنسي للأطفال لأغراض تجارية وغير تجارية؛
وفي سنة 2008 جاء المؤتمر العالمي الثالث ريوديجانيرو لمتابعة وتقييم عمل نتائج المؤتمرات السابقة، ويلاحظ أن خطة عمل ريوديجانيرو شددت على وضع الدول لاستراتيجية شاملة تتضمن مجموعة من القوانين والسياسات والتنظيمات والخدمات الضرورية من كافة القطاعات ولاسيما قطاعات الرعاية الاجتماعية والتعليم والصحة والأمن والعدالة، وذلك لغرض مساندة اجراءات المنع ومجابهة الخطر. أنظر، المركز الصحفي، اختتام الملتقى العالمي لمكافحة الاستغلال الجنسي للأطفال والمراهقين بالبرازيل، موجود على الموقع https://www.unicef.org/arabic/protection/24267_46560.html تاريخ التصفح 2020/04/04 على الساعة 11:03 ؛
اتفاقية مجلس أوربا لحماية الأطفال من الاستغلال والاعتداء الجنسي عقدت ووقعت في 25 أكتوبر 2007 في لانزاروت (اسبانيا) والملفت للانتباه على هذه الاتفاقية أنه بالرغم من أنها تخص فقط دول مجلس أوروبا، إلا أنه بإمكان أي دولة في العالم الدخول إليها وتعتبر تونس الدولة من بين الدول التي انضمت للاتفاقية في 03 يناير 2018 (أنظر، الموقع
(https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/201/signatures.

حيث تأتي في صدارة هذه النصوص الاتفاقية الدولية الخاصة بحماية حقوق الطفل والتي اعتمدتها الجمعية العامة للأمم المتحدة في 20 نوفمبر 1989 ودخلت حيز التنفيذ في 02 سبتمبر 1990 أين بلغ عدد الدول الموقعة عليها آنذاك 61 دولة"[1].

حيث تطرقت هذه الاتفاقية إلى جريمة استغلال الطفل عبر شبكة الأنترنت في المادة 34 بنصها على " تتعهد الدول الأطراف بحماية الطفل من جميع أشكال الاستغلال الجنسي والانتهاك الجنسي، ولهذه الأغراض تتخذ الدول الأطراف بوجه خاص جميع التدابير الملائمة الوطنية والثنائية والمتعددة الأطراف لمنع:

1/حمل أو اكراه الطفل على تعاطي أي نشاط جنسي غير مشروع؛

2/الاستخدام الاستغلالي للأطفال في دعارة أو غيرها من الممارسات الجنسية غير المشروعة؛

3/الاستخدام الاستغلالي للأطفال في العروض والمواد الداعرة".

ولأن هذه الجريمة آثارها خطيرة على صحة ونفسية الطفل والتي قد تقوده إلى حد فقدان احترام ذاته ألزمت هذه الاتفاقية في المادة 39 الدول باتخاذ جميع التدابير اللازمة، والمناسبة لتشجيع التأهيل البدني والنفسي وإعادة الإدماج الاجتماعي للطفل الذي يكون ضحية أي شكل من أشكال الإهمال، والاستغلال بجميع أنواعه، كما أوصت بأن يجرى هذا التأهيل في بيئة تعزز صحة الطفل واحترامه لذاته وكرامته.

ونظرا لمحدودية الاتفاقية السابقة في مجال الجرائم المعلوماتية المتعلقة ببغاء الأطفال، جاء البروتوكول الاختياري لاتفاقية حقوق الطفل المتعلق ببيع وبغاء واستغلال الأطفال في المواد الإباحية والذي دخل حيز النفاذ في 18 يناير 2002[2] حيث كان من بين أهم الأسباب التي

---

[1]- الحاج علي بدر الدين، الحماية الجنائية للطفل في القانون الجزائري، مذكرة ماجستير، جامعة تلمسان، 2010/2009، ص.06.وغني عن البيان أن الجزائر قد صادقت على هذه الاتفاقية مع التصريحات التفسيرية بموجب المرسوم الرئاسي رقم 461/92 المؤرخ 19 ديسمبر 1992 (الجريدة الرسمية رقم 91).

[2]- صادقت عليه الجزائر بموجب المرسوم الرئاسي رقم 229/06 المؤرخ في 02 سبتمبر 2006، الجريدة الرسمية رقم 55.

أدت بإصداره هو القلق الدولي لحجم انتشار استغلال الأطفال في البغاء والمواد الإباحية، وانتشار معها السياحة الجنسية للأطفال خاصة في الدول الآسيوية[1].

حيث تعرف الفقرة الفرعية ج من المادة 02 من هذه البروتوكول استغلال الأطفال جنسيا عبر الانترنت بأنه " تصوير أي طفل بأي وسيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل لإشباع الرغبة الجنسية أساسا".

طبعا هذا الاستغلال إما أن يتضمن اتصالا جسديا (كالاغتصاب مثلا) أو قد لا يتضمن اتصالا جسديا كمشاهدة الأطفال في أوضاع معينة أو تشجيعهم أو تهديدهم على التصرف بطرق جنسية شاذة.

ويشير هنا الدليل الاسترشادي للجمعيات الأهلية ومنظمات المجتمع المدني أن هناك 03 أشكال أساسية متصلة بالاستغلال الجنسي التجاري للأطفال وهي[2] :

-بغاء الأطفال: أين يجبر الطفل لممارسة البغاء من قبل أشخاص بالغين في مقابل حصوله على احتياجات أساسية كالنقود أو للسماح بالمرور عبر الحدود إلى أماكن آمنة محظورة عليهم، وقد ساعد على انتشار البغاء بين الأطفال ظهور الانترنت وما حمله من مواد إباحية والمتمثلة في تصوير للطفل يمارس نشاطا جنسيا أو عن طريق المحاكاة لإشباع الرغبة الجنسية[3]؛

-المواد الإباحية: وتشير إلى أي نوع من أنواع العروض بأي وسيلة كانت يستخدم فيها الطفل للقيام أو محاكاة أفعال جنسية باستخدام أجهزة الكمبيوتر كما في حالة ما إذا كانت الأنترنت أداة الجريمة.

-الاتجار: وهنا تجدر الإشارة إلى أن نسبة كبيرة من الأطفال الذين يتم تهريبهم عادة ما يتم استغلالهم جنسيا.

---

[1]- غالية رياض نبشة، حقوق الطفل بين القوانين الداخلية والاتفاقيات الدولية، ط.01، منشورات الحلبي الحقوقية، لبنان، 2010، ص.335-336.

[2]- أنظر، الموقع :

https://www.ecpat.org/wpcontent/uploads/2016/04/protecting_children_from_csec_in_disaster_arb.pdf

تاريخ التصفح: 2020/04/04 على الساعة 14:00.

[3]- خالد مصطفى فهمي، المرجع السابق، ص.79.

وكان من بين التوصيات التي أوصى بها هذا البروتوكول ما جاء في مادته الثالثة من أن " تكفل الدولة الطرف أن تغطي، كحد أدنى الأفعال والأنشطة التالية تغطية كاملة بموجب قانونها الجنائي سواء كانت هذه الجرائم ترتكب محليا أو دوليا أو كانت ترتكب على أساس فردي أومنظم... انتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالطفل على النحو المعرف في المادة 02 أعلاه".

ثالث نص يحضرنا في هذه الدراسة هي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1] والتي انعقدت في 2010/12/21 بالقاهرة تهدف الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات ، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها، حيث نصت في المادة 12 على تعريف جريمة الإباحية على أنها انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات. كما شددت العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر، ويشمل التشديد حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

ولأن أهم ما يترتب على الانضمام لهذه الاتفاقيات الدولية هو التزام الدولة بمواءمة وموافقة القوانين الوطنية مع هذه الاتفاقيات، حيث تتمتع هذه الأخيرة بأولوية في التطبيق والنفاذ وذلك استنادا إلى نظرية سمو القانون الدولي على القانون الداخلي، ناهيك عن عدم جواز أي طرف عضو في أحد هذه الاتفاقيات الاعتذار بنصوص قانونه الداخلي ليبرر عدم وفائه بالتزاماته

[1]- انضمت الجزائر إلى هذه الاتفاقية العربية بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 8 سبتمبر 2014، الجريدة الرسمية رقم 57.
يمكن تصفح بنود هذه الاتفاقية على الموقع التالي:
https://ar.wikisource.org/wiki/%d8%a7%d9%84%d8%a7%d8%aa%d9%81%d8%a7%d9%82%d9%8a%d8%a9_%d8%a7%d9%84%d8%b9%d8%b1%d8%a8%d9%8a%d8%a9_%d9%84%d9%85%d9%83%d8%a7%d9%81%d8%ad%d8%a9_%d8%ac%d8%b1%d8%a7%d8%a6%d9%85_%d8%aa%d9%82%d9%86%d9%8a%d8%a9_%d8%a7%d9%84%d9%85%d8%b9%d9%84%d9%88%d9%85%d8%a7%d8%aa
تاريخ التصفح 2020/04/04 على الساعة 17:37.

الدولية، فيا ترى هل تتواءم نصوصنا الجزائية الداخلية الخاصة بحماية القصر من الاستغلال الجنسي عبر الانترنت مع التزاماتنا الدولية التي انضممنا إليها؟.

ما يمكن ملاحظته بصفة أولية عن طريق مسح عام لمجمل هذه النصوص العقابية أن المشرع الجزائري حاول إفراد سياسة جزائية خاصة بحماية عرض الأطفال[1]، معتمدا في ذلك على سن الضحية، بحيث جعل منها (السن) أحيانا ظرفا مشددا في بعض جرائم العرض كما هو الحال في جريمة اغتصاب طفلة لا تتجاوز 18 سنة[2] أو في حالة الفعل المخل بالحياء بغير عنف على قاصر لم يكمل 16 سنة[3] أو جريمة الشذوذ الجنسي الواقعة على قاصر لم يكمل 18 سنة[4] وكذا في حالة جريمة تحريض الأطفال على الدعارة[5] ، وأحيانا أخرى ارتقى بها كركن أساسي لا تقوم الجريمة إلا بتوافرها ومثالها جريمة الفعل المخل بالحياء بدون عنف على قاصر لم يكمل 16 سنة[6] وكذا جريمة تحريض الطفل على الفسق وفساد الأخلاق[7].

وعلى غرار باقي التشريعات العربية والغربية أصدر المشرع الجزائري القانون رقم 04/09 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[8] والذي رغم أهميته خاصة في المجال المعلوماتي كون أنه يهدف أساسا إلى الوقاية من الجرائم المعلوماتية إلى أننا باستقرائنا لنصوصه لم نجد أي مادة تجرم أو تعاقب عن الاستغلال الجنسي للأطفال عبر هذه الوسائل.

كما أن هذا القانون لم يتوسع في نطاق المسؤولية الجزائية لمقدمي الأنترنت، خاصة أنه ليس له الرقابة والإشراف الكامل على مستخدمي الخدمة التي يقوم بتزويدها إليهم بما فيهم فئة الأطفال، فهو يكتفي على الغالب الأعم بتوصيل خدمته، والتأكد من تشغيل الشبكة بكفاءة.

---

[1]- لأكثر تفصيل، راجع الحاج علي بدرالدين، المرجع السابق، ص.64 وما يليها.

[2]- المادة 336 الفقرة 2 ق.ع.

[3]- المادة 335 ق.ع.

[4]- المادة 338 الفقرة 02 ق.ع.

[5]- المادة 344 ق.ع.

[6]- المادة 334 ق.ع.

[7]- المادة 342 ق.ع.

[8]- القانون رقم 04/09 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47.

وعليه بقيت هذه الحماية تقليدية لا تخدم مقتضيات التجريم فيما يتعلق ببغاء الأطفال على الأنترنت إلى أن تم تعديل قانون العقوبات سنة 2014[1] والذي استحدث نص المادة 333 مكرر 1 والتي جاء فيها " يعاقب بالحبس من 05 سنوات إلى 10 سنوات وبغرامة من 500.000 دج إلى 1000.000 دج كل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر.

أول ما يمكن ملاحظته على هذا النص هو توحيد المشرع لسن الطفولة المشمول بالحماية وهو 18 سنة وذلك تماشيا مع اتفاقية الأمم المتحدة لحماية الأطفال التي وسعت دائرة الحماية إلى غاية 18 سنة، وهو مسعى يحمد عليه المشرع، إلا أن ما يؤخذ على هذا النص هو عدم تحديد المشرع العقابي للوسائل المرتكبة بها هذه الأفعال، تاركا السلطة التقديرية للقاضي وكان حريا به أن يخص الاستغلال الجنسي عن طريق الأنترنت بنصوص خاصة[2]، وعلى سبيل المقارنة نجد أن المشرع المصري قد نص صراحة في المادة 116 مكرر أ من قانون الطفل رقم 126 لسنة 2008 على تجريم استخدام الأنترنت أو الحاسب الآلي لممارسة الأفعال الاباحية ضد القصر[3].

---

[1]- القانون رقم 01/14 المؤرخ في 04 فبراير 2014 يعدل ويتمم قانون العقوبات، الجريدة الرسمية رقم 07. الشيء الملاحظ هنا أنه أضاف كذلك جريمة أخرى تتعلق بالمتاجرة في الأطفال لأي غرض من الأغراض وهو الفعل المنصوص عليه في المادة 319 مكرر والتي تنص على " يعاقب بالحبس من 05 سنوات إلى 15 سنة وبغرامة من 500.000 دج إلى 1500.000 دج كل من باع أو اشترى طفلا دون سن 18 سنة لأي غرض من الأغراض وبأي شكل من الأشكال، ويعاقب بنفس العقوبات كل من حرض أو توسط في عملية بيع الطفل. إذا ارتكبت الجريمة جماعة إجرامية منظمة أو كانت ذات طابع عابر للحدود الوطنية، تكون العقوبة السجن من 10 سنوات إلى 20 سنة وغرامة من 1000.000 دج إلى 2000.000 دج. ويعاقب على الشروع بنفس عقوبات الجريمة التامة".

[2]- حتى المادة 347 ق.ع جاءت بنفس السياق في معرض تجريمها لفعل إغراء الأشخاص بقصد التحريض على الفسق، وذلك باستخدامها في نهاية المادة عبارة " بأي وسيلة أخرى"

[3]- القانون منشور على الموقع :
https://www.egyptiantalks.org/invb/topic/74451%d9%82%d8%a7%d9%86%d9%88%d9%86%d8%a7%d9%84%d8%b7%d9%81%d9%84%d8%a7%d9%84%d9%85%d8%b5%d8%

ما يمكن ملاحظته أيضا بخصوص نص المادة 333 مكرر 1 أن هناك أكثر من صورة يتحقق بها النشاط المكون للركن المادي للجريمة والتي يدخل ضمنها فعل التصوير، انتاج، نشر، توزيع، ترويج، استيراد، تصدير، عرض، بيع، حيازة مواد إباحية تتعلق بقصر. مع ملاحظة أن ما تضمنته هذه المادة من تعداد لصفات المستغلين لعناصر السلوك الاجرامي السابقة إنما هي أمور واردة على سبيل المثال لا الحصر حيث إنه في ظل العولمة وثورة الاتصالات قد تشهد جرائم الاستغلال الجنسي للأطفال أنماطا وصورا أخرى مستحدثة غير المنصوص عليها في هذه المادة.

وبصدور القانون رقم 12/15 المتعلق بحماية الطفل[1] جدد المشرع الجزائري حمايته للأطفال المستغلين جنسيا في المواد الإباحية حيث اعتبر من بين الحالات التي تعرض الطفل للخطر إذا كان ضحية الاستغلال الجنسي للطفل بمختلف أشكاله من خلال استغلاله لاسيما في المواد الإباحية وفي البغاء وإشراكه في عروض جنسية.

ودعم ايضا هذه الحماية حتى في مجال الإعلام وذلك بنصه في المادة 10 من نفس القانون بمنع استعمال الطفل في ومضات اشهارية أو أفلام أو صور أو تسجيلات مهما كان شكلها إلا بترخيص من ممثله الشرعي وأن يكون ذلك خارج فترات التمدرس وهذا تحت طائلة المتابعات الجزائية.

وقد أفرد المشرع في هذا القانون نصوص خاصة بحماية القصر من الابتزاز والنيل من الحياة الخاصة، حيث نص في المادة 140 منه على " يعاقب بالحبس من سنة إلى 03 سنوات وبغرامة من 150.000 دج إلى 300.000 دج كل من ينال أو يحاول النيل من الحياة الخاصة للطفل بنشر أو بث نصوص و/أو صور بأية وسيلة يكون من شأنها الاضرار بالطفل".

وبذات العقوبة نص أيضا في المادة 141 من نفس القانون على معاقبة كل من يستغل الطفل عبر وسائل الاتصال مهما كان شكلها في مسائل منافية للآداب العامة والنظام العام، وهذا دون الاخلال بالعقوبات الأشد.

---

b1%d9%%d8%a7%d9%84%d9%85%d8%b9%d8%af%d9%84%d8%a8%d8%a7%d9%84%d9%82%d8%a7%d9%86%d9%88%d9%86-126-%d9%84%d8%b3%d9%86%d8%a9-2008

تاريخ التصفح: 2020/04/05 على الساعة 07:15.

[1]- القانون رقم 12/15 المؤرخ في 15 يوليو 2015 يتعلق بحماية الطفل، الجريدة الرسمية رقم 39.

ثانيا: تقييم التجربة الجزائرية في مكافحة جرائم الاستغلال الجنسي للأطفال عبر الأنترنت

ما يمكن ملاحظته من خلال تقييم التجربة الجزائرية في مجال حماية الأطفال من الاستغلال الجنسي عبر الأنترنت أن المشرع الجزائري حاول بسط أكبر قدر من الحماية للقصر وذلك من خلال النصوص التقليدية لقانون العقوبات أو حتى من خلال التعديلات التي أجريت عليه، كما أنه دعم هذه الحماية من خلال اصداره لقانون حماية الطفل.

لكن تبقى هذه الحماية التي تفرضها النصوص القانونية غير كافية في مواجهة الاستغلال الجنسي للأطفال في صورته التقليدية والمستحدثة ولا سيما في مواجهة التقنية العالمية والإنترنت ،والتي قد تعرض الطفل للانحراف،أو أن يكون الطفل محلا لهذا الاستغلال الجنسي ،وتمثل بالتالي اعتداء ماديا ومعنويا على سلامة الأطفال وحقهم في ملكية صورهم والاستغلال المالي لها الأمر الذي يستلزم أن يصدر المشرع قوانين قادرة على المواءمة مع هذه التقنية والإلمام بجميع مظاهر هذه الجريمة.

وفيما يتعلق بالحماية التي منحها المشرع الجزائري من خلال المادة 333 مكرر 01 من قانون العقوبات أو حتى المادة 141 و143 من قانون حماية الطفل يعاب عليها أنها جاءت ناقصة كون أنها لا تجرم الاطلاع العمدي والتنزيل العمدي للمواد الإباحية للأطفال، كون أن الاعتداء على الأطفال يتجدد كلما تم تحميل أو اطلاع على هذه الفديوهات أو الصور أو المواقع الإباحية، وهو ما يمكن المجرمين من الإفلات من العقاب، كما أن المشرع لم يقم بتجريم فعل الاستمالة أو المراودة باعتبارهما الخطوة الأولى لاستدراج الطفل عبر الأنترنت واستغلاله جنسيا.

كما أن التجربة الجزائرية تفتقر نوعا ما إلى التدابير الوقائية والتي هي المفتاح في نظام حماية الأطفال كون أنها تهدف أساسا إلى تجنب الضرر قبل وقوعه أو التخفيف من آثاره في حالة العكس. هذه التدابير الوقائية التي نرى أنها يجب أن تخدم ثلاثة أوجه:

الوجه الأول: وهو يستلزم بالضرورة توفير الخدمات الجيدة لكل فئات المجتمع بما فيهم فئة الأطفال[1] وذلك تجنبا لنشوء مثل هذه الممارسات غير الشرعية، فأغلبية علماء النفس والاجتماع يجمعون على أن أهم أسباب استغلال الأطفال جنسيا عدم احتواء المناهج الدراسية

---

[1]- تنص المادة 05 في فقرتها 03 على أن " تقدم الدولة المساعدة المادية اللازمة لضمان حق الطفل في الحماية والرعاية"

على أساليب التربية الجنسية التي تماشى والمرحلة العمرية للطفل فضلا عن ذلك صعوبة الظروف المعيشية وحالات الفقر.

الوجه الثاني: وهو الذي يرتكز على فئة الأطفال المعرضين للخطر كون أن هذه الفئة كي الأكثر عرضة للاستغلال الجنسي بجميع صوره بما فيها عن طريق الأنترنت، وهنا يأتي الدور على المفوض الوطني لحماية الطفولة من أجل وضع برامج وطنية ومحلية لحماية الطفولة من الاستغلال الجنسي، وكذا وضع نظام معلوماتي وطني كما جاء في القانون حول وضعية الطفل في الجزائر بالتنسيق مع الإدارات والهيئات المعنية.

الوجه الثالث: يستهدف الجناة و/ أو الأطفال الضحايا، وذلك للحد من آثار الانتهاك من ناحية وهنا يجب تفعيل نص المادة 06 من قانون حماية الطفل والتي تنص على أن" تكفل الدولة حق الطفل في الحماية من كافة أشكال الضرر أو الإهمال أو العنف أو سوء المعاملة أو الاستغلال أو الإساءة البدنية أو المعنوية أو الجنسية، وتتخذ من أجل ذلك كل التدابير المناسبة لوقايته وتوفير الشروط اللازمة لنموه ورعايته والحفاظ على حياته وتنشئته تنشئة سليمة وآمنة ...".

الخاتمة

في ختام هذه الدراسة يمكن القول أن المشرع الجزائري أنه سعى إلى استحداث نصوص قانونية جديدة لمكافحة جرائم الاستغلال الجنسي للأطفال عبر الأنترنت ، لكنه لم يتوسع كثيرا كما رأينا في مجال الحماية، حيث أن التطور التقني الذي نعيشه اليوم ضف إلى ذلك الذكاء الذي يتميز به الجناة يحتم علينا سن نصوص قانونية جديدة تستوعب أي تطور قد يحدث في طرق استغلال الأطفال في المواد الإباحية خاصة عبر شبكة الأنترنت.

وفي هذا الصدد نوصي بضرورة حجب المواقع الإباحية نهائية وتأمين شبكات الأنترنت فالوقاية خير من العلاج وذلك لمنع الأطفال من الانحراف الجنسي عبر الأنترنت؛

وكذلك يجب إثارة مسؤولية مزودي خدمات الأنترنت ومزودي الإيواء عن المحتويات غير المشروعة سيما تلك التي لها علاقة مباشرة أو غير مباشرة ببغاء الأطفال.

ومن جهة أخرى يجب الاهتمام بالجانب الوقائي كما أسلفنا الذكر كون أنه يهدف إلى معالجة الأسباب الحقيقية التي تجعل المنحرفين يقبلون على مثل هذه الجرائم وكذلك بالنسبة للقصر لفهم الدوافع التي أثرت عليهم وجعلتهم يرضخون لهذه الإغراءات.

نافلة القول أن الدور الأساسي يقع على الأسرة ممثلة في الوالدين اللذان يقع عليهما دور التوعية وملاحظة الطفل باستمرار ومتابعة طريقة لعبه، كما تتطلب العملية تأهيلا نوعيا لرجال الضبطية للتحقيق في مثل هذا النوع الحساس من الجرائم المعلوماتية .

حماية الأطفال من الاستغلال في المواد الإباحية عبر الانترنت في التشريع الجزائري

Protect children from being exploited in Internet pornography in Algerian legislation

د. طالب (م) حمّــاس هديات
أستاذة محاضرة (أ)
كلية الحقوق و العلوم السياسية
جامعة أبي بكر بلقايد – تلمسان - الجزائر

مقدمة

إن الله عز وجل قد خلق الإنسان و كرمه، و جعله خليفته في الأرض ليعمرها و يسعى في مناكبها، ورزقه من الطيبات، ولم يتركه هملا ، بل بين له سبل الحق و دروب النجاة في شتى أوجه حياته . و لما فطرت نفس الإنسان على حب اللذائذ و الشهوات فإن الله عز وجل قد بين له الطريق القويم لإشباع تلك الشهوات.

فالغريزة الجنسية لدى الإنسان تعتبر حقا من حقوقه، لهذا سعى الإسلام إلى تنظيمها و توجيهها وذلك عن طريق العلاقة الشرعية ألا وهي الزواج، و ذلك صيانة للأعراض و حماية للأنساب. إلا أن النفس الأمارة بالسوء، قد تدفع بالبعض إلى الإنحراف عن سبيل الرشد ، وبالتالي إتيان أنماط شتى من الممارسات الجنسية الشاذة . فالإعتداء الجنسي من أخطر الجرائم التي يمكن أن تصيب الإنسان، وتشكل خطورة أكبر إذا ما أصابت الطفل ،سواء تمت مباشرة على جسمه أو بصفة غير مباشرة .

ونظرا أن العالم اليوم يشهد تقدما تكنولوجيا متسارعا، أدى إلى ظهور جرائم خطيرة ترتكب عبر الأنترنت تستهدف هذه الفئة الضعيفة والمتمثلة في الأطفال.و من بين هذه الجرائم استغلال الطفل في المواد الإباحية، والتي تعتبر من أخطر الجرائم لأنها تسعى من جهة إلى تحقيق المنفعة المادية وذلك بوضع الطفل كسلعة تباع وتشترى عبر الانترنت من خلال استغلاله في الصور الإباحية، ومن جهة أخرى ترتب له آثار سلبية نفسية و سلوكية وخيمة والتي تمتد إلى كبره. ومن المشكلات التي تثيرها جرائم الأنترنت بصفة عامة أنها تتسم بسرعة تنفيذها، وسهولة إخفاء

الأدلة من قبل المجرم و محو آثارها مما يصعب القبض عليه، بالإضافة إلى كون هذه الجريمة عابرة لحدود الدولة فقد تتوزع عبر أقاليم عدة دول مما يعيق إجراءات المتابعة و المحاكمة.هذا ما دفع التشريعات الجزائية ، من بينها التشريع الجزائري إلى تجريم هذه الظاهرة و الحد منها.

فالإشكالية التي تطرح في هذا الموضوع تمثل في : ما المقصود باستغلال الأطفال في المواد الإباحية عبر الانترنت ؟ وما مدى فعالية التشريع الجزائري في حماية الأطفال من هذه الأفعال؟ للإجابة على هذه الإشكالية قسمنا الموضوع إلى نقطتين نتطرق في الأولى إلى مفهوم استغلال الأطفال في المواد الإباحية عبر الانترنت و أركانه،و في النقطة الثانية إلى آليات حماية الطفل من هذه الجريمة .

أولا : مفهوم استغلال الأطفال في المواد الإباحية عبر الانترنت و أركانه

تصنف جرائم الاعتداء على العرض إلى صنفين الأولى ترتكب مباشرة على جسم الطفل كالاغتصاب، و الفعل المخل بالحياء. و الصنف الثاني يتمثل في ذلك الاعتداء الذي لا يقع مباشرة على جسم الضحية و إنما يسخره لمختلف أشكال سوء المعاملة الجنسية كالتحريض على الدعارة و فساد الأخلاق من جهة ،ومن جهة أخرى إلى استخدامه في العروض و المواد الإباحية و هو الذي يهمنا في هذه الدراسة .

1- مفهوم استغلال الأطفال في المواد الإباحية عبر الانترنت

يقصد بالاستغلال الجنسي للأطفال بصفة عامة ، كل تصرف جنسي من قبل شخص بالغ موجه إلى الطفل ، مجبرا إياه على القيام بأفعال ذات بعد جنسي أو تشجيعه على القيام بهذه الأفعال أو التوسط فيها أو استغلالها عن طريق النشر، أو التوزيع بأي شكل من الأشكال، بهدف الحصول على إشباع جنسي للبالغ أو لتحقيق المنفعة المادية 1.

ويعتبر استغلال الأطفال في المواد الإباحية عبر الانترنت أحد صور الاستغلال الجنسي للأطفال، يهدف إلى تحقيق أغراض تجارية، و يعتمد وسائل تقنية كثيرة أين يظهر الطفل وهو يمارس أنشطة جنسية، حقيقية أو محاكية، أو تكشف بعض أجزاء جسمه بشكل فاحش يجعله يثير الرغبة أو اللّذة الجنسية، وقد يتعلق الأمر بطفل أو عدة أطفال يقومون بأنشطة جنسية بصفة

[1]- نوايسه نانسي خالد سليم، جريمة الاستغلال الجنسي للأطفال عبر الانترنت- دراسة مقارنة- ، جامعة عمان العربية، الأردن، 2011 ، ص 22.

فردية أو مع طفل أو عدة أطفال، أو عرض صور الأطفال عراة أو شبه عراة في صفحات مثيرة هدفها جعل الطفل بضاعة جنسية.

وهذا ما نصت عليه المادة 2 الفقرة "ج" من البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال و استغلال الأطفال في البغاء و في المواد الإباحية[1] على أن :

"يقصد باستغلال الأطفال في المواد الإباحية تصوير أي طفل بأي وسيلة كانت يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل لإشباع الرغبة الجنسية أساسا."

يتبين لنا من خلال هذا التعريف أن مفهوم استغلال الأطفال في المواد الإباحية يتكون من مجموعة من العناصر تتمثل فيما يلي :

المواد الإباحية عبارة عن تصوير مرئي لطفل أو أكثر بأية وسيلة كانت.

أن يظهر هذا التصوير أعضاء جنسية للطفل أو نشاط جنسي يشترك فيه الطفل.

يستوي أن يكون هذا التصوير حقيقيا أو افتراضيا أو بالمحاكاة.

2- أركان استغلال الأطفال في المواد الإباحية

إن جريمة استغلال صورة الطفل في المواد الإباحية، جريمة خطيرة لماترتبه من تدمير للطفل و تفقده لكل حاسة أخلاقية.

و لقد نص المشرع الفرنسي على هذه الجريمة في المادة 227-22-1 من قانون العقوبات و عاقب كل من يقوم باقتراحات جنسية لقاصر باستعمال وسيلة الاتصال الإلكتروني، و ترفع العقوبة إذا نتج عن هذه الاقتراحات عقد لقاء مع القاصر.

و بالتالي يمكن اعتبار جريمة استغلال صورة قاصر جريمة تمهد لجرائم جنسية أخرى قد تقع في المستقبل.

---

[1]-البروتوكول المعتمد بموجب قرار الجمعية العامة للأمم المتحدة رقم 54 /263 المؤرخ في 2000/05/25 – صادقت عليه الجزائر بموجب المرسوم الرئاسي رقم 06 -299 المؤرخ في 2006 /09/02 ، الجريدة الرسمية المؤرخة في 2006/09/06 ، العدد 55.

كما حدد المشرع الفرنسي من خلال المادة 227-23 و 227 – 24 الأفعال المخلّة بالآداب العامة للطفل، و المتمثلة في إرسال أو بث أو تسجيل صور ذات طبيعة إباحية أو جنسية للأطفال[1].

أما بالنسبة للتشريع الجزائري فنصت المادة 141من قانون حماية الطفل[2] على أن : "من دون الإخلال بالعقوبات الأشد، يعاقب .... كل من يستغل الطفل عبر وسائل الاتصال مهما كان شكلها في مسائل منافية للآداب العامة و النظام العام."

فهذا النص جاء بتجريم واسع و شامل حيث لم يبين هذه الوسائل بصفة دقيقة و منه فقد تشمل وسائل الاتصال الإلكتروني و غير الإلكتروني، كما أنه لم يحدد لنا الأفعال المنافية للآداب و النظام العام.إلاّ أن المشرع الجزائري أحالنا إلى نص المادة 333 مكرر 1/1 من قانون العقوبات[3] أين حدد هذه الأفعال كما يلي : "يعاقب .... كل من صوّر قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية، أو صوّر الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر."

فالباعث على تجريم هذه الأفعال هو الرغبة في مكافحة استغلال صورة الصغير. فالتجريم هنا، ليس مناطه الاعتداء على الطفل لأنه لم يقع بعد، و إنما ينصرف إلى سلوك الجاني الذي يركز في مشروعه الإجرامي على استغلال الطفولة عن طريق استعمال و ترويج صور جنسية أو ذات طابع جنسي تخص الأطفال[4].

---

[1]-Anne Sophie CHAVENT – LECLERE – La lutte contre la cyberpornographie enfantine : évolutions de la loi française – Revue pénitentiaire et de droit pénal – Cujas – Octobre – Décembre 2008 – N°4 – p 789 - 790.

[2]- قانون رقم 15-12 المؤرخ في 15يوليو 2015 المتعلق بحماية الطفل ، الجريدة الرسمية المؤرخة في 19يوليو 2015 العدد 39.

[3]-الأمر رقم 66 - 156 المؤرخ في 08/ 06 /1966 المتضمن قانون العقوبات المعدل و المتمم بقانون رقم14-01 المؤرخ في 04 فبراير 2014

[4]- مدحت رمضان -جرائم الإعتداء على الأشخاص و الأنترنت - دار النهضة العربية -القاهرة - مصر - 2000 - ص 141؛ إبراهيم عيد نايل - الحماية الجنائية لعرض الطفل من الإعتداء الجنسي - دراسة مقارنة - دار النهضة العربية - القاهرة - 2001 ص 43.

يتضح من المادة 333مكرر 1السابقة الذكر وجوب توافر الأركان التالية :

الركن المفترض

يتمثل في سنّ الطفل الضحية و الذي حدده المشرع الجزائري بأقل من 18 سنة[1]، و سواء كان ذكرا أو أنثى.

ب- الركن المادي

يتحقق الركن المادي بتوافر أحد الأفعال المنصوص عليها في المادة 333 مكرر 1/1 و المتمثلة في التصوير، إنتاج، توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع مواد إباحية.

فإنتاج أو توزيع أو نشر المواد الإباحية قبل ظهور الانترنت، كان نوعا ما صعبا يكلف صاحبه مخاطر كبيرة وتكبده نفقات عالية فيما يخص التعامل في هذه المواد و السعي للعثور عليها و الانتفاع بها. أما مع ظهور الانترنت وشيوعها فأصبح الأمر يسيرا و بأقل التكاليف بسبب التطور المستمر لوسائل الإنتاج و الاستعمال.

ب.1 – إنتاج، توزيع، أو نشر الصور الإباحية

قد يتحقق سلوك الجاني بتصوير الطفل في وضعيات داعرة أو بإنتاج هذه الصور أو يوزعها أو ينشرها.

و يشمل إنتاج الصور الإباحية الرسوم على الصور الفتوغرافية و الإلكترونية و الأفلام والإعلانات و الصور المعدلة على الكمبيوتر. و لا تهم الطريقة التي تم بها التصوير سواء بالكاميرات الرقمية أو العادية أو الفيديو[2] أو بأي من البرامج المتوفرة عبر الانترنت.

كما ذكر المشرع أن التصوير قد يتضمن الأعضاء الجنسية للطفل، أو يتضمن أنشطة جنسية يقوم بها القاصر بصفة حقيقية أو خيالية. فلا يتعلق التجريم في هذه الحالة بالاعتداء على الطفل وإنما يتعلّق بسلوك الفاعل الذي يهدف إلى إفساد و تشويه صورة الطفولة، فالغرض الرئيسي من التجريم هو محاربة انجذاب البالغين تجاه الأطفال جنسيا و الذي يتحقق بصورة واقعية أو خيالية[3].

---

[1]- المادة 2 /1 من قانون حماية الطفل .

[2]- بسام عاطف المهتار - إستغلال الأطفال (تحديات و حلول) الطبعة الأولى - منشورات الحلبي الحقوقية - س لبنان - 2008- ص65.

[3]- أكمل يوسف السعيد يوسف - الحماية الجنائية للأطفال من الإستغلال الجنسي - دار الجامعة الجديدة – الإسكندرية - 2014- ص283.

أمّا التوزيع فيقصد به تسليم تلك الأشياء لعدد من الأفراد بغير تمييز. نلاحظ أن المشرع الفرنسي وفقا للمادة 227-23 السابقة استعمل مصطلحات "البث" و" التسجيل" و "الإرسال" وحسن ما فعل لأنها تنطبق على الأفعال التي تتم عبر الانترنت، أما مصطلح "التوزيع" الذي جاء به المشرع الجزائري فيستعمل لـمّا يتعلق الأمر عادة بالمجلات أو المطبوعات الورقية .

و بالنسبة للنشر، فقد يتم في مواقع مختلفة عبر شبكة الانترنت ، لتمكين الجمهور من مشاهدتها.

ب.2- ترويج الصور أو الاستيراد أو التصدير أو العرض أو البيع ، و الحيازة

كما يتحقق الركن المادي بترويج هذه الصور الإباحية أو استيرادها أو تصديرها أو عرضها أو بيعها. الترويج هو عبارة عن مجموعة من الأنشطة التي تهدف إلى التواصل مع العملاء أو الجمهور، وذلك من أجل نشر الوعي حول منتج معين، مما يحفز العملاء على شراء هذا المنتج ورفع قيمته وتمييزه عن غيره . وهنا المقصود بهذا المنتج الصور الإباحية للأطفال.

و يقصد بالاستيراد إدخال سلعة أو خدمة مشروعة للبلاد بطريقة قانونية.فقد يتم استيراد المواد الإباحية تحت اسم سلعة مشروعة إذ أن الدولة لا ترخص باستيراد مثل هذه المواد[1]. أما التصدير فهو اخراج هذه المواد من الدولة الأصلية إلى دول أخرى. و هذا ما يمكن تحقيقه بكل سهولة عن طريق الانترنت.

و يقصد بالعرض وضع الرسم أو الإعلان أو الصورة أو الفيلم أو أي شيء مخل بالحياء عرضة للأنظار، حيث يمكن أن يراها كل من يدخل الموقع عبر الشبكة. كما يمكن أن ترسل صور لأطفال تتضمن صورا إباحية لأشخاص آخرين عبر الشبكات الالكترونية [2].

أي يكون الطفل في هذه الحالة هدفا للاستغلال ومادة له في آن واحد، فخرجات الإنتاج سواء كانت صورا أو مقاطع فيديو للأطفال، توجه إلى أطفال آخرين عبر شبكة الانترنت أي أن الهدف هنا هو إيصال المنتج إلى أطفال آخرين[3].

---

[1]-عبد الحكم فودة – الجرائم الماسة بالآداب العامة و العرض في ضوء الفقه و قضاء النقض- دار الكتب القانونية - مصر- 2004- ص441.

[2]-أسامة بن غانم العبيدي- جريمة استغلال الجنسي للأطفال عبر الانترنت ،دراسة مقارنة- مجلة الشريعة والقانون- كلية القانون-الإمارات العربية المتحدة- العدد 53 - ص 88 .

[3]-أسامة أحمد المناعسة ، جلال محمد الزعبي – جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة) – دار الثقافة – الأردن – 2014 – ص 263.

و أما بيع الأشياء المخلة للحياء فهي نقل ملكيتها مقابل ثمن معين، أي في هذه الحالة لا يمكن للشخص الإطلاع على الموقع إلا بعد دفع مبلغ معين.

أما حيازة المواد الإباحية فتعني تلك السيطرة المادية التي يتمتع بها الشخص بصفته مالكا أو مستعيرا أو مستأجرا أو تحت أي وصف آخر. ويعد الشخص حائزا على هذه المواد إذا ضبطت في مسكنه أو هاتفه النقال أو موقعه الإلكتروني أو صفحة التواصل الاجتماعي الخاصة به[1].

والهدف من تجريم حيازة المواد الإباحية هو رغبة المشرع في إحاطة الطفل بحماية أوسع و وقايته من كل استغلال جنسي، ذلك أن حيازة هذه الصور و مشاهدتها تعتبر بمثابة استمالة و تشجيع للجوء إلى الاستغلال الجنسي للأطفال.

ج- الركن المعنوي

يعتبر استغلال صورة القاصر جريمة عمدية تتطلب علم الجاني بأنه يقوم بفعل من الأفعال السابقة المكونة للركن المادي، و أن تتجه إرادته إلى ارتكاب هذا السلوك الإجرامي[2]. و لقد اشترط المشرع الجزائري قصد خاص يتمثل في تحقيق غرض جنسي، أي أن تصوير الجاني للأعضاء الجنسية للقاصر يكون لغرض إشباع الغرائز الجنسية سواء لحسابه أو لحساب أشخاص آخرين وهذا ما يفهم من عبارة "..... أو صوّر الأعضاء الجنسية للقاصر لأغراض جنسية أساسا ......"،و من هنا لا تحقق الجريمة في حالة ما إذا كان الغرض من القيام بهذه الأفعال طبي كالتقارير الطبية أو خبرة طبيةّ شرعية، ومحاضر الشرطة و التي تعتبر من حالات الإباحة المنصوص عليها في المادة 29 من قانون العقوبات الجزائري.

ثانيا: آليات حماية الأطفال من الاستغلال في المواد الإباحية عبر الانترنت

إن قانون حماية الطفل لعام 2015 اعتبر الطفل الذي يتعرض للاستغلال الجنسي بما في ذلك الاستغلال في المواد الإباحية عبر الانترنت، في دائرة الأطفال المعرضون للخطر[3]، وبالتالي يتعين توفير الحماية اللازمة له وهو ما عمل على تحقيقه من خلال هذا القانون.فأقر عقوبات جزائية لكل

---

[1]-طارق سرور - جرائم النشر و الإعلام - الجزء 1 - دار النهضة العربية - مصر - 2008 – ص 502.

[2]-أسامة بن غانم العبيدي - المرجع السابق- ص 89 .

[3]- أنظر المادة 2/2 من قانون حماية الطفل.

من يتعدى على الطفل.كما أقر إجراءات علاجية إذا تبين أن الطفل قد وقع في خطر. ومن أجل وقاية الطفل من هذا الاستغلال لابد من إتباع الإجراءات الوقائية، وهذا ما سوف نتطرق إليه تبعا.

1- الآليات العقابية و العلاجية

تعني الآليات العقابية أو الزجرية، العقوبات التي يتم توقيعها على الجاني مرتكب الجريمة في حق الطفل، أما الآليات العلاجية فهي التي تخص الطفل الذي وقع ضحية جريمة من أجل التكفل به.

الآليات العقابية

لقد أقر المشرع الجزائري عقوبات جزائية للأشخاص الذين يستغلون الأطفال طبقا للمادة 141 من قانون حماية الطفل، فرغم أن هذه المادة أفردت الطفل بحماية خاصة من جريمة الاستغلال في المواد الإباحية عبر الانترنت، حينما أكدت على تجريم استغلالهم في الأفعال المخلة بالحياء والمنافية للآداب العامة .إلا أنها وضعت حكما محيرا يدفع للشك حيث تضمنت بعض التناقض في العقوبة ، فحددتها بالحبس من سنة إلى ثلاث سنوات وبغرامة مالية من 150.000 دج إلى 300.000 دج، فهي عقوبة مختلفة عن العقوبة الواردة في المادة 333 مكرر1/1 من قانون العقوبات و المتمثلة في الحبس من 5 إلى 10 سنوات و غرامة تقدر من 500000إلى 1000000دج. و الخاصة بمرتكبي الجرائم بحق الأطفال ومن ضمنها استغلالهم إباحيا عبر الانترنت.

فبالرجوع للمادة 141 من قانون الطفل المذكورة أعلاه فإن المشرع الجزائري استهلها بعبارة "دون الإخلال بالعقوبات الأشد ..." أي أنه يحيلنا إلى المادة 333 مكرر 1 من قانون العقوبات فيما يخص استغلال الأطفال في المواد الإباحية عبر الانترنت[1]. لكن ما الجدوى من إقرار عقوبتين مختلفتين لنفس الجريمة ؟ فكان على المشرع أن يقوم بتوحيد العقوبة لإزالة أي لبس. و ربّما

[1]- أنظر المادة 143 من قانون حماية الطفل التي تنص على أن :" يعاقب على الجرائم الأخرى الواقعة على الطفل، لاسيما الاستغلال الجنسي للطفل ، و استعماله في البغاء وفي الأعمال الإباحية ،........طبقا للتشريع الساري المفعول و لاسيما قانون العقوبات ."

اعتبر الأفعال التي شملتها المادة 141 أقل خطورة من تلك الواردة في المادة 333 مكرر 1، لهذا كان عليه تحديد تلك الأفعال بطريقة واضحة.

يالإضافة إلى العقوبة الأصلية ، لقد أقر المشرع الجزائري عقوبة تكميلية متمثلة في مصادرة الوسائل المستعملة لارتكاب الجريمة.[1]

في حين لقد خصص المشرع المصري لجريمة استغلال الأطفال في المواد الإباحية عقوبة الحبس لا تقل عن سنتين و بغرامة لا تقل عن 10000 جنيه و لا تجاوز 50000 جنيه، و هذا طبقا للماد 116 مكرر أ من قانون الطفل رقم 126لسنة 2008.[2]

و أقر المشرع الفرنسي عقوبة الحبس لمدة 5 سنوات و بغرامة 75000 أورو ، و ترفع العقوبة إلى سبع سنوات حبس و 100000 أورو في حالة ما إذا تم النشر إلى جمهور غير محدد أو في حالة ما إذا تم عن طريق شبكة الإتصالات الالكترونية طبقا للمادة 227-22 من قانون العقوبات[3]. كما نص المشرع الفرنسي من خلال المادة 227-28 على معاقبة الشخص المعنوي على هذا النوع من الجرائم ، إن المشرع الجزائري هو أيضا أقر المسؤولية الجزائية لمزودي ومقدمي خدمة الانترنت وفقا للقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4]. لكن نص عليها بصفة عامة أي لم يحط الطفل بحماية خاصة في مجال استغلاله في المواد الإباحية.

الآليات العلاجية

إذا تعرض الطفل لأخطار تهدد حياته أو صحته البدنية أو النفسية أو تهدد عرضه و أخلاقه أو تربيته،بما في ذلك الاستغلال في المواد الإباحية فيكون بحاجة إلى حماية،خاصة إذا عجزت الأسرة

---

[1]-أنظر المادة 333 مكرر 2/1 من قانون العقوبات الجزائري .

[2]- أكمل يوسف السعيد يوسف -المرجع السابق- ص277.

[3]- Valérie MALABAT – Droit Pénal Spécial – 5ème Edition – Dalloz – 2011 – N°374 – p 179.

[4]- تنص المادة 12 " زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه يتعين على مقدمي خدمات "الإنترنت" ما يأتي:

ب - وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها."

على تقديمها.لهذا لقد جعل المشرّع الجزائر يحماية الطفل على درجتين : حماية اجتماعية ترتكز أساسا على التعاون مع الأسرة لإخراج الطفل من دائرة الخطر و التي تعتبر الأصل،وتكون عن طريق هيئات وطنية و أخرى محلية [1] و حماية قضائية [2] و هي حماية استثنائية يتكفل بها قضاة الأحداث. فالحماية الاجتماعية هي حماية وقائية، حيث تعتبر جهازا لإنذار المبكر عن الأخطار التي تهدد الطفل في نفسه و تربيته. فهدفها هو مد يد المساعدة للأسر من أجل إبعاد الطفل عن الخطر. تتكفل بها الهيئة الوطنية لحماية وترقية الطفولة على المستوى الوطني، و مصالح الوسط المفتوح على المستوى المحلي. و تلتزم هذه المصالح بمجرد إخطارها بالسهر على سلامة الأوضاع المادية و المعنوية لحياة الأطفال، فتراقب على وجه الخصوص صحتهم و تربيتهم و أخلاقهم، كما تقوم بمختلف الفحوصات و الأبحاث اجتماعية للوقوف على شخصية الأحداث من أجل إيجاد أحسن طريقة لتأهيله و مساعدته.

إن مهمة مصالح الوسط المفتوح البحث عن اتفاق رضائي مع الممثل الشرعي لاتخاذ أفضل تدبير يخدم مصلحة الطفل [3]. لكن إذا تعذر عليها ذلك ترفع الأمر إلى قاضي الأحداث و تصبح حماية قضائية، أين يتعين على قاضي الأحداث اتخاذ التدابير اللازمة، وهذا ما تناولته المادة 35 من قانون حماية الطفل كإبعاد الطفل عن مقره الأسري إذا كان هذا المقر مصدرا للخطر [4].

إن استغلال الطفل في المواد الإباحية عبر الانترنت قد لا يقتصر فقط على إفساد أخلاق الطفل و صورته، وإنما قد ينتهي باعتداء جنسي فعلي عليه إذا ما تم عقد لقاءات معه. ومن هنا لقد استحدث المشرع إجراء خاص للتحقيق مع الطفل ضحية اعتداء جنسي وسماع شهادته، يتمثل في إجراء التسجيل السمعي البصري [5].

---

[1]- نص المشرع على الحماية الاجتماعية من المادة 11 إلى 31 من قانون حماية الطفل .

[2]- نص على الحماية القضائية من المادة 31 إلى 45 من قانون حماية الطفل.

[3]- نجيمي جمال – قانون حماية الطفل في الجزائر : تحليل و تأصيل – الطبعة الثانية – دار هومة – الجزائر – 2016 – ص 64.

[4]- كحث الطفل من طرف الوالدين على مشاهدة أفلام أو عروض إباحية أو ترويج له هذه الأفعال ، فهذا يؤثر على نفسيته و يفسد أخلاقه .

[5]- تنص الفقرة الأولى من المادة 46 من قانون حماية الطفل على أن :" يتم خلال التحري و التحقيق، التسجيل السمعي البصري لسماع الطفل ضحية الاعتداءات الجنسية".

فمن الأهداف الأساسية التي يرمي إليها إجراء التسجيل السمعي البصري هو تسهيل سماع الطفل بقدر ما أمكن وذلك بتجنيبه إعادة و تكرار ما حدث له، فبتكرار الرواية سوف يعيش معاناته مرات أخرى و بالتالي قد يدخل في صدمات إضافية1. فتسجيل شهادة الطفل يعتبر دليل إثبات هام حيث يتم سماعه أثناء الجلسات، و في مواجهة المتهم أيضا دون الحاجة إلى حضور الطفل واستجوابه مرات عديدة. وكذا لتفادي الاتصال المباشر بين الطفل و الجاني.

2- الآليات الوقائية

على الرغم من المقتضيات الزجرية الهامة التي تقر عقوبات رادعة في حق الجناة، فإن هذا النوع من الجرائم لا زال منتشرا داخل المجتمعات نظرا لظهور شبكة الانترنت و اتساع استخدامها عالميا إذ أصبح هذا النشاط أكثر انتشارا ممّا يجعل السيطرة عليه أمراً في غاية الصعوبة.

فحماية الطفل من هذه الجرائم عن طريق الزجر بعقوبات سالبة للحرية للجناة ، لا يعتبر الحل الوحيد و الأمثل لردع هؤلاء الجناة. و إنّما يجب التفكير في حلول أخرى وقائية كتوعية الطفل و تحسيسه بمخاطر وسائل الإعلام و خاصة الانترنت وفرض رقابة من طرف الأسرة بصفة خاصة و المدارس و المؤسسات التعليمية بصفة عامة.

فالأنترنت و كذا التلفزيون لهما تأثير فعال و سلبي على الطفل، فتتبعهما لا يتطلب من المشاهد سوى أقل مجهود عقلي. و لهذا انعدام وسائل الرقابة تجعل الطفل يتتبع برامج مصبوغة بطابع العنف و الهيجان الجنسي بالتالي تترك أثرها عليه.

لأن الطفل في هذه المرحلة غير قادر على التميز بين النافع و الضار و لا يستطيع فهم هدف و غاية بعض البرامج فيؤمن بالشيء المرئي المحسوس المتمثل في الصورة و يحاول تقليده، كما أن إدمانه على مواقع الانترنت هذا الفضاء الموسع للاتصال و الذي دخل كل البيوت، يحمل انعكاسات خطيرة بعيدة على الهدف المسطر في التسلية و الترفيه. فقد يؤدي إلى اكتشافات تهدد صلب الأسرة إذا ما غابت المتابعة و المراقبة.

لهذا يجب تحذير الأبناء من إعطاء معلومات شخصية عن أنفسهم لأشخاص عن طريق الأنترنت، و تحذيرهم أيضا من عقد لقاءات مع أشخاص تم التعرف عليهم عبر الأنترنت.

---

[1]- Gérard Raymond, Droit de l'enfance et de l'adolescence, 5ème Edition, Litec, 2006, N° 555, p 284.

كما وجب تأمين شبكة الانترنت لمنع العصابات المنظمة، و مجرمي الشذوذ الجنسي من اختراق بعض المواقع التي يقبل عليها الأطفال، وتعد هذه الوسيلة وقائية وطريقة غير مباشرة لحماية الحدث من استغلال المنظمات الإجرامية عن طريق اختراق هذه الشبكات، لهذا وجب على الشركات و المؤسسات الحكومية أو الخاصة بتأمين شبكاتها ضد الاختراق و بذلك تقوم بحماية نطاقها المعلوماتي بحيث لا يسهل الوصول إليه، أو يقوم بها الوالدين أو كل من له سلطة قانونية على الطفل[1].

لابد من استخدام أنظمة حماية برامج تتيح للآباء معرفة المواقع التي زارها الأبناء،أو تمنعهم تلقائيا من الدخول إلى المواقع المحظورة عن طريق التشفير ومنع التصفح غير المرغوب.

وتماشيا مع حماية الطفل في مجال الإعلام،لقد منحه المشرع الجزائري حماية من خلال المادة 34 من قانون الإعلام[2] بأن تحترم النشريات و الدوريات القوانين المتعلّقة بالطفولة و الآداب العامة،إلا أنه لم يأت بقواعد فيما يخص استعمال شبكة الانترنت من طرف الأطفال.

و من هنا لقد وضع القانون الفرنسي بعض الإجراءات الوقائية و هذا منذ 2001 و ذلك تماشيا مع الاتفاقية الأوروبية لمكافحة جرائم الحاسب الآلي و الانترنت و التي تناولت 4 أنواع من الجرائم من بينها الجرائم المتعلقة بالمواد الإباحية للأطفال (الإنتاج أو النشر غير المشروع للمواد الإباحية و صور الأطفال الفاضحة، فوضعت بعض التدابير من بينها حث الدول الأعضاء على تجريم كل فعل يقصد من وراءه نشر أو اكتساب أو حيازة المواد الإباحية المتعلقة بالأطفال عن طريق نظام الحاسب الآلي. كما أضاف المشرع الفرنسي، وفقا لقانون 2007/03/05 مادتين 706-35-1 و 706-47-3 ضمن قانون الإجراءات الجزائية تمثل في إنشاء وسيلة تحقيق خاصة تسمح للمحققين من رجال الشرطة القضائية التسرب عبر الاتصال الإلكتروني، لإمكانية القبض على المتهم في الجرائم الالكترونية الماسة بالأطفال خاصة الجرائم الجنسية[3].

---

[1]- بودبة سعيدة – الاستغلال الجنسي للأطفال عبر الانترنت – مجلة البحوث و الدراسات القانونية و السياسية – جامعة الأغواط – الجزائر العدد 13- 2016 - ص 99 .

[2]- قانون رقم 12-05 المؤرخ في 2009/01/12 و المتعلّق بقانون الإعلام.الجريدة الرسمية المؤرخة في 2009/01/15 – العدد 2.

[3]-Philippe BONFILS, Adeline GOUTTENOIRE – Droit des mineurs – 1ère édition , Dalloz, 2008 – N° 1807 – p 1061 .

و من جهة أخرى لقد قيدت الولايات المتحدة الأمريكية الدخول إلى بعض المواقع الممنوعة للأطفال من خلال تحققها من سن الزوار و يتم هذا التحقق عن طريق بعض التقنيات كإدخال بطاقة هوية أو إدخال كلمة السر[1]. كما وضعت إنجلترا عدة أنظمة، أدخلت من خلالها مسؤولية مزود خدمة الانترنت فيعرض لعقوبات مدنية أو جزائية إذا قام بتسهيل المحادثات أو الاتصالات بين الأشخاص محبي الجنس مع الأطفال و الأطفال - عن طريق إظهارهم على الشبكة أو استضافتهم فيها - حيث اعتبرت هذا المزود كوسيط بين المجرم و الطفل عبر الانترنت[2].

خاتمة

تعتبر جريمة استغلال الأطفال في المواد الإباحية عبر الانترنت ظاهرة عالمية، فنشر وعرض المواد الإباحية عبر شبكة الأنترنت باستخدام التقنية الرقية،على فئة كبيرة من المستهلكين بصرف النظر عن أعمارهم و جنسهم تجعل الأطفال عرضة أخطار جسدية ونفسية ترتب لهم آثار ترافقهم مدى الحياة.

لهذا لابد من تضافر كافة الجهود من أجل حماية الأطفال من خطر هذه الجريمة، بدءا بالأسرة ثم المدرسة و المجتمع.

فرغم توفير المشرع الجزائري للطفل حماية جنائية واسعة في هذا المجال من خلال قانون العقوبات وقانون حماية الطفل، إلا أن هذه الحماية تعتبر غير كافية حيث تعتريها عدة معيقات، ترجع أساسا في كون هذه الجريمة لا تسلط مباشرة على جسد الطفل وإنما تستغل جسده بغرض تحقيق نفع مادي . وبالتالي تطرح مشاكل إجرائية كبيرة لاسيما في مجال الاختصاص، و في صعوبة اثبات الجريمة نظرا لغياب الأدلة المادية، بالإضافة إلى أن المجرم المعلوماتي يتميز عن المجرم العادي كونه محترف، متخصص و ذكي. فيستطيع أن يعبث بالبيانات أو يغيرها أو يمحوها في وقت قياسي. ضف إلى ذلك الكم الهائل لهذه البيانات التي تعد عائقا أمام سلطات البحث و التحقيق. الأمر

---

[1]-Andrew JOINT, Field Fisher WATERHOUSE - Protecting children from pedophiles on the Internet - Computer Law & Security - Elsevier Science - Vol. 19 N° 1 - 2003 – p 44 – 48.

[2]-Andrew JOINT – Règlementation relative aux chatrooms en ligne – Protection des enfants contre la pédophilie sur internet – Editions Scientifiques et médicales – Elsevier – Vol. 58 – Jan – Mai 2003 – N°1-2 – p 11 – 15.

الذي يستوجب تكوين شرطة متخصصة في مكافحة الجرائم المعلوماتية،واتباع إجراءات خاصة في هذه الجرائم كالإستعانة بخبراء في مجال البرمجة و بمهندسين في الصيانة و الاتصالات.

دون أن ننسى الدور الوقائي المتمثل في توعية الطفل من طرف الوالدين وتعليمه المفهوم الصحيح للأنترنت، وتحذيره من أخطارها بالنصح والتوجيه عبر المواقع النافعة و المفيدة وحثه على تجنب المواقع غير مرغوب فيها ؛ وتفعيل دور المدرسة في مراقبة والتصدي لهذه الظاهرة مع مشاركة الهيئات الاجتماعية والمدنية.

كما يجب مراقبة مواقع الانترنت وخاصة مواقع التواصل الاجتماعي، وما يعرض فيها و محاولة إيجاد وتفعيل آليات الحظر على المواقع الإباحية حتى لا يسهل و لوج الأطفال لهذه المواقع.

جريمة التحرش الالكتروني بالقصر – آليات الردع ومدى مجابهتها للظاهرة-

Crime of electronic harassment of minors - deterrence mechanisms and their response to the phenomenon

بن طاع الله زهيرة باحثة سنة ثالثة دكتوراه تخصص قانون قضائي
كلية الحقوق والعلوم السياسية (19 مارس 1962)
جامعة جيلالي اليابس، سيدي بلعباس، الجزائر

مقدمة:

لقد أدى التطور السريع لتكنولوجيات الإعلام والاتصال والانفتاح الواسع على استخدامها بشكل غير عقلاني حول العالم، إلى تهيئة البيئة الخصبة التي ساهمت في زيادة تفشي الجرائم المرتكبة بواسطة هذه التقنية. بحيث سخرت للجناة تحقيق مآربهم الإجرامية، وهذا لعدة أسباب يمكن إرجاعها لسهولة ارتكاب هذا النوع من الجرائم الذي يعتمد على وسائل ذات طابع تقني، بالإضافة إلى سهولة تخفي الجاني الذي يتمتع بثقافة الكترونية وتقنية تساعده في إخفاء معالم جريمته مما يصعّب من عملية التوصل إليه في بعض الأحيان[1].

وتعتبر جريمة التحرش الالكتروني أحد صور الجريمة المعلوماتية التي لم تعد تقتصر على الأشخاص البالغين فقط، وإنما امتدت لتستهدف الشريحة العمرية الأصغر من مستخدمي شبكة الانترنيت. ونظرا للآثار الشنيعة التي مست هذه الفئة الضعيفة تسارعت الجهود الدولية لحماية الأطفال القصر من هذه الجريمة الشنيعة، عن طريق إرساء الأطر القانونية اللازمة لمكافحة الجريمة وردع مرتكبيها لأن لا محدودية الشبكة المعلوماتية لا يعني عدم الكشف عن الجناة ومتابعتهم لتطبيق القوانين ضدهم[2]. وهذا على غرار اتفاقية حقوق الطفل لسنة 1989

---

[1]- أيمن أحمد زيتون، "التحرش عبر الانترنيت: الإشكاليات والمواجهة"، مجلة القراءة والمعرفة، جامعة عين شمس، كلية التربية، العدد 206، ديسمبر 2018، ص: 205.

[2]- في تصرح السيد **ميك موران** رئيس وحدة الإنتربول المعنية بمكافحة جرائم الاستغلال الجنسي للأطفال جاء فيه :" يقال إن الإنترنت لا يعرف حدودا، ولكن هذا لا يعني أن القوانين لن تُطبَّق وأنه لن يتم الكشف عن الأشخاص الذين يرتكبون الجرائم عبر الإنترنت. فما من ملاذ آمن لا تُكشف فيه هوية الأفراد الذين يعتقدون أن بإمكانهم الاتجار بصور الاستغلال الجنسي للأطفال عبر الإنترنت أو نشرها. هذا ما أثبتته مجددا العملية التي

والبروتوكول الاختياري الملحق بها بشأن بيع الأطفال واستغلالهم في المواد الإباحية[1] واتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي[2]، وكذا اتفاقية بودابست الخاصة بالجرائم الواقعة ضد شبكات الحاسب الآلي لسنة 2001 والتي خصصت في نصوصها دراسة لأشكال التحرش الجنسي بالأطفال عبر شبكات الحاسب الآلي.

وفي هذا السياق وفي محاولة لمواجهة تفاقم جريمة التحرش بالأطفال عبر الانترنيت من جهة ومواكبة للجهود الدولية المبذولة كان لزاما على التشريعات العقابية الداخلية وضع ترسانة من القوانين لتوفير الحماية اللازمة للقصر من جرائم التحرش الالكتروني، وهو ما يضعنا ونحن بصدد هذا المقال أمام إشكالية رئيسية مفادها **ما مدى مواجهة التشريع الجزائري لجريمة التحرش الالكتروني للقصر أمام تطور الجريمة وثبات النصوص القانونية؟**

من هذا المنطلق، وفي محاولة للإجابة عن الإشكالية الرئيسية اعتمدت الدراسة على المنهج التحليلي المقارن والذي يتناسب مع موضوعها، وهذا من خلال من خلال تسليط الضوء على ماهية جريمة التحرش الالكتروني بالقصر بوصفها "**جريمة العصر القاتلة بكاتم الصوت**"[3]، والتي تختلف عن الجريمة التقليدية من حيث صور وأشكال هذه الجريمة. وما مدى ملائمة أو قصور النصوص القانونية الوطنية التصدي لهذه الجريمة من خلال آليات الردع التي كفلتها مقارنة بالتشريعات العربية.

بناء على ذلك، فلقد تم تضمين الورقة البحثية العناصر الآتية:

ينبغي أن توجهّ تنبيها إلى المجرمين الآخرين مفاده أنه سيتم الكشف عنه". نقلا عن موقع الانتربول الالكتروني: https://www.interpol.int/ar/1/1/2012/18 مطلع عليه بتاريخ : 2020/02/24 على الساعة 23:01.

[1]- اعتمدت اتفاقية حقوق الطفل من قبل الجمعية للأمم المتحدة سنة 1989 و ودخلت حيز التنفيذ بتاريخ 2 سبتمبر 1990، والبروتوكول الاختياري الملحق بها بشأن بيع الأطفال واستغلالهم في البغاء وفي المواد الإباحية، والذي اعتمد وعرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 263 الدورة الرابعة والخمسون المؤرخ في 25 ماي 2000 ودخل حيز النفاذ في 18 جانفي 2002.

[2]- ووقعت في 25 أكتوبر 2007 في مدينة لانزروت باسبانيا ودخلت حيز التنفيذ في 1 جويلية 2010.

[3]- لقد جرى استعمال هذه العبارة في تصريح للخبيرة الاستشارية في مجال استخدام الانترنيت المجتمعي "هناء الرملي"، بمناسبة اليوم العالمي لحماية الطفل من الإساءة والإيذاء في 19 و 20 نوفمبر في إطار اليوم العالمي للطفل. أنظر: نايلة الصليبي، "ما هي ظاهرة التنمر الإلكتروني أو الاستقواء الإلكتروني في اليوم العالمي لحماية الطفل من الإساءة والإيذاء؟" مقال منشور بتاريخ 2018/11/22، عبر الموقع الالكتروني: **https://www.mc-doualiya.com/chronicles/email-mcd**

- المحور الأول: الإطار المفاهيمي لجريمة التحرش الالكتروني بالقصر
- المحور الثاني: آليات الردع المقررة لجريمة التحرش الالكتروني بالقصر

المحور الأول: الإطار المفاهيمي لجريمة التحرش الالكتروني بالقصر والموقف القانوني منها

مع انتشار وسائل المعلومات والاتصال والانفتاح عليه بشكل هائل لم تعد احتمالية تعرض الشخص للتحرش الجنسي مرتبطة بالمقابلة المباشرة بين المتحرش والضحية، بل أصبح بإمكان المتحرش الوصول إلى ضحيته في أي وقت وفي أي مكان. وهذا ما يجعل جريمة التحرش الالكتروني جريمة معلوماتية بامتياز، خرجت عن لباسها التقليدي لتصبح جريمة مستحدثة تعجز التشريعات في بعض الأحيان عن ردعها وهذا راجع لافتقارها نصوصا قانونية تتواءم والطبيعة الخاصة لجريمة التحرش الالكتروني.

وتتفاقم جرائم التحرش الالكتروني بالأطفال في العالم فبعد أن وصل عدد الأطفال المتحرش بهم عبر الانترنيت سنة 2017 عدد 246 مليون طفل حسب ما صرحت به منظمة اليونسكو، فإنه وفي سنة 2019 ووفقا لتقرير أصدرته منظمة اليونيسيف والممثل الخاص للأمين العام للأمم المتحدة المعني بالعنف ضد الأطفال رصدت فيه حسب إحصاء شمل 30 بلد أن طفل واحد من كل ثلاثة أطفال وقع ضحية للتحرش الكتروني، وأن واحد من بين خمسة أطفال أعلنوا أنهم لم يذهبوا للمدارس بسبب التحرش والعنف عبر الانترنيت[1].

وفيما يلي توضيح لجريمة التحرش الالكتروني، من خلال محاولة التقريب في البداية إلى مفهوم الجريمة التحرش الالكتروني من خلال تسليط الضوء على الجريمة المعلوماتية باعتبارها أعم **(أولا)**، بالإضافة إلى أشكال التحرش الالكتروني **(ثانيا)**.

أولا: التعريف بجريمة التحرش الالكتروني بالقاصر

إن ظاهرة التحرش عبر الانترنيت عرفت أوصافا كثيرة للدلالة عليها كالتحرش الافتراضي والتحرش عن بعد والتحرش السبيراني، ومهما اختلفت المفردات فإنها تلتقي للدلالة عن كل سلوك غير لائق له طبيعة جنسية يضايق الضحية فيؤثر على سلوكياتها وحالتها النفسية[2].

---

[1]- https://www.unicef.org/fr/communiqu%C3%A9s-de-presse/un-tiers-des-jeunes-de-30-pays-victimes-harcelement-en-ligne, visité le 18/01/2020 à 19:15.

[2]- هدى أحمد ديب ومحمود عبد العليم محمد سليمان، "إيذاء النساء: باثولوجيا التحرش الجنسي الالكتروني بالمرأة"، مجلة جيل للعلوم الإنسانية والاجتماعية، مركز جيل البحث العلمي، العدد 42، ماي 2018، ص: 132.

من هذا المنطلق، فإن دراسة جريمة التحرش الالكتروني باعتبارها جريمة مركبة انتقلت من طبيعتها التقليدية المعروفة في التشريعات العقابية -التحرش الجنسي- إلى جريمة متطورة ساهمت البيئة المعلوماتية على توفير الجو وهذا من خلال العناصر الآتية:

1- ماهية الجريمة المعلوماتية

وهي صنف جديد من الجرائم التي ظهرت بفعل ثورة المعلومات والاتصالات، بحيث ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى الكترونية. وتتعدد المصطلحات المستخدمة للتعبير عن هذه الجريمة الناشئة في بيئة نظم المعلومات، فابتداء من مصطلح إساءة استخدام الكمبيوتر ومرورا بمصطلح جرائم الكمبيوتر والجرائم التقنية وغيرها إلى جرائم المعلوماتية *Cyber crime*.[1]

ولحداثة الجريمة قد عالج المشرع الجزائري في البداية نوعا من أنواع الجرائم المعلوماتية وهي جرائم الماسة بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات بموجب القانون 04-15[2]، وفي سنة 2009 تدارك المشرع النقص وأصدر أول نص قانوني لمكافحة الجرائم الالكترونية بموجب القانون رقم 09-04[3] الذي ورد في 06 فصول تضمن الفصل الأول منه أحكام عامة بإعطاء مفهوم للمصطلحات المستعملة[4]، فعرف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنها تلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة ﭬي قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية[5].

---

[1]- أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، 2014، ص: 84.

[2]- القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 1966/06/08 والمتضمن قانون العقوبات الجزائري، جريدة رسمية عدد 71 لسنة 2004.

[3]- القانون رقم 09-04 المؤرخ في 2009/08/05 والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47 لسنة 2009.

[4]- بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة، 2011/2010، ص: 04.

[5]- أنظر المادة 02 من القانون 90-04 السالف الذكر.

انطلاقا مما سبق، يتضح أن المشرع الجزائري قد وسع من نطاق تجريم مثل هذه الأفعال، فلم يضبط الجريمة المعلوماتية في نوع محدد تحسبا للتطور التكنولوجي والتقني في المستقبل، وحتى يبقى وصف الجريمة المعلوماتية يجمع كل اعتداء أو مساس يقع عن طريق شبكة المعلوماتيات[1].

هذا وتتميز الجريمة المعلوماتية بجملة من الخصائص والسمات التي تميزها عن الجريمة التقليدية بصفة عامة، فالطابع الدولي الذي يخص الجريمة المعلوماتية يجعل القواعد القانونية التقليدية عاجزة عن مجابهتها وتقفي آثر مرتكبيها، كما أن استهداف هذا النوع من الجرائم للمعلومات وليس الماديات وذلك باستعمال وسائل وتقنيات معقدة ومتطورة يعسر من إثباتها.

وجدير بالإشارة أن المشرع الجزائري لم يتطرق لا في قانون العقوبات ولا في القانون 09-04 إلى تعداد الجريمة المعلوماتية ولو على سبيل المثال، على عكس المشرع المصري الذي عددها في 24 نوعا بموجب القانون رقم 175 الصادر بشأن مكافحة جرائم تقنية المعلومات[2].

[1]- و بحسب تقرير للاتحاد الدولي للاتصالات بشأن الإطار القانوني لحماية الأطفال من مخاطر الشبكة المعلوماتية ووسائل تقنية المعلومات وبخاصة الجرائم الالكترونية " إطار قانوني إقليمي بشأن حماية الأطفال على الانترنيت : دليل المنطقة العربية "، جاء فيه تعريف للجريمة الالكترونية على أنها: " أي فعل ينطوي على استخدام تقنية المعلومات أو نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة الكترونية أو تكنولوجية أخرى بطريقة غير مباشرة بما يخالف أحكام القانون"، منشور في الموقع الالكتروني: Presence/ArabStates/Documents/Reports/Guidelines_and_Model_Law.pdf

-https://www.itu.int/en/ITU-D/Regional

، تاريخ الإطلاع : 2020/02/17 على الساعة 14:39.

[2]- القانون المصري رقم 175 المؤرخ في 2018/08/14 المتعلق بمكافحة جرائم تقنية المعلومات، جريدة رسمية عدد 32 مكرر لسنة 2018. وتتعلق بالجرائم التالية:جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها- جريمة الدخول غير المشروع- جريمة تجاوز حدود الحق في الدخول- جريمة الاعتراض غير المشروع-جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية- جريمة الاعتداء على البريد الالكتروني أو المواقع أو الحسابات الخاصة- جريمة الاعتداء على تصميم موقع-جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة-جريمة الاعتداء على سلامة الشبكة المعلوماتية-جريمة الإضرار غير العمدي بسلامة الشبكة العنكبوتية- جريمة تداول البرامج والأجهزة والمعدات المستخدمة في ارتكاب الجرائم-جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الالكتروني-الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الالكتروني-جرائم الاعتداء على القيم وحرمة الحياة الخاصة والمحتوى غير المشروع-جريمة ربط المعلومات الشخصية للغير بمحتوى مناف للآداب أو ماس بالشرف والاعتبار- جريمة إنشاء وإدارة المواقع بقصد ارتكاب جريمة، جريمة إخفاء أو العبث بالأدلة من قبل مسئول الموقع، جريمة تعمد تعريض الأنظمة المعلوماتية لجريمة من قبل مسئول الموقع-جريمة الإهمال من قبل مسئول الموقع الذي يؤدى إلى تعريض الأنظمة المعلوماتية

2- جريمة التحرش الجنسي بالقاصر

وهي جريمة تمس بكرامة الإنسان وحريته وتتداعى أثارها على سلوكياته وتصرفاته، وقد استخدم المصطلح لأول مرة من قبل الباحثة ماري روي في تقرير كتبته سنة 1973 قدمته إلى معهد ماساتشوستش للتكنولوجيا (***MIT***) بالولايات المتحدة الأمريكية عن الأشكال المختلفة لقضايا عدم المساواة بين الجنسين[1].

وينصرف مفهوم التحرش الجنسي إلى كل إثارة يتعرض لها جسد الضحية عن عمد من خلال إزالة الثياب عليه وكشف عورته أو التلصص واستراق النظر عليه أو تعريضه لأعمال مشينة غير أخلاقية كإجباره على التلفظ بعبارات جنسية أو على التقاط صور إباحية له .

وتعرفه الأمانة العامة للأمم المتحدة على أنه: " كل ما هو غير مرحب به من تلميح جنسي أو طلب أداء خدمة جنسية أو سلوك إيماءة لفظية أو جسدية ذات طابع جنسي أو أي سلوك ذو طابع جنسي يمكن اعتباره أو توقعه منطقيا كسبب لإهانة الآخرين وإذلالهم ..."[2].

هذا وجدير بالملاحظة أن جريمة التحرش الجنسي بالطفل شأنها شأن الاستغلال الجنسي من الجرائم العمدية الواقعة على الأطفال، إلا أن الاستغلال الجنسي وإن كان ينصرف إلى استغلال الطفل واستخدامه لممارسة سلوك جنسي من قبل المعتدي، فإن التحرش يتميز باستخدام أساليب متنوعة إما لفظية أو بصرية أو حتى رمزية ذات دلالات جنسية قد تتطور لتشكل استغلالا جنسية. ليكون بذلك التحرش الجنسي أحد صور الاستغلال الجنسي المرتكبة ضد الأطفال.

وباعتبار محور الدراسة إنما يخص الضحايا من فئة الأطفال، فإنه لا بد من البحث عن مفهوم الطفل، والبحث عن السن أو المرحلة العمرية اللازمة لتوفير الحماية القانونية له؟

لجريمة- جريمة امتناع مقدم الخدمة عن تنفيذ قرار محكمة بالحجب-جريمة عدم محافظة مقدم الخدمة على سرية البيانات-جريمة امتناع مقدم الخدمة عن تنفيذ القرار الصادر من جهة التحقيق المختصة- جرائم إخلال مقدم والخدمة بتنفيذ الالتزامات التي نص عليها القانون-جريمة عدم إبلاغ المسؤول عن الشخص الاعتباري لتعرضه لجريمة معلوماتية .

[1]- هشام عبد الحميد فرج، التحرش الجنسي وجرائم العرض، دار الوثائق، القاهرة، 2011، ص: 19.

[2]- نقلا عن : سحر فؤاد مجيد، "جريمة التحرش الجنسي بالأطفال عبر الانترنيت (دراسة في القانون الأمريكي والعراقي)"، المجلة الأكاديمية للبحث القانوني، عدد خاص، 2017، ص: 305.

إن بدايات المناداة بحقوق الأطفال كانت سنة 1923 أين تبلورت مجموعة من المبادئ التي تكفل حقوق الطفولة، والتي اعتمدتها الجمعية العامة للأمم المتحدة سنة 1955 كأهداف لم تنتج أثارها القانونية إلى غاية 1959 أين اعتمدت الجمعية العامة إعلان حقوق الطفل، وفي الأخير صدرت الاتفاقية الأكثر أهمية والمعروفة باتفاقية حقوق الطفل لسنة 1989 والتي أرست مبادئ دولية في مجال مناهضة حقوق الطفل وحمايتها. وتعتبر أول اتفاقية عرفت مصطلح "الطفل"[1] بشكل صريح وواضح في نص المادة الأولى، والتي جاء فيها: " كل إنسان لم يتجاوز سن 18 سنة ما لم يبلغ سن الرشد قبل ذلك بموجب القانون المطبق عليه".

أما في التشريع الوطني فلم يستقر المشرع الجزائري على مصطلح موحد في مختلف قوانينه بحيث تعددت التسميات للدلالة على صغير السن، فكانت أولى التسميات هي" القاصر" ونص عليها بموجب المادة 49 من قانون العقوبات فقسمها إلى مرحلتين: مرحلة ما قبل بلوغ سن التمييز المحدد بـ 13 سنة ومرحلة ما بين سن 13 سنة وسن 18 سنة، ثم اصطلح "الحدث" في كل من قانون الإجراءات الجزائية وقانون تنظيم السجون[2].

وبعد صدور قانون حماية الطفل بموجب القانون 15-12[3] استعمل لأول مرة مصطلح "الطفل"، حيث تضمنت المادة الثانية منه تحديد مفاهيم بعض المصطلحات فعرف الطفل على

---

[1]- يعرف علماء النفس الطفولة على أنها تلك المرحلة العمرية من دورة حياة الإنسان الممتدة من مرحلة الميلاد إلى بداية المراهقة، ويقسمون مراحل الطفولة إلى 04 مراحل كالآتي: مرحلة الرضاعة (Infancy) التي تبدأ من الميلاد إلى بلوغ سن الثانية من عمر الطفل، مرحلة الطفولة المبكرة (Early childhood) وتبدأ من سن الثانية إلى سن السادسة من العمل، مرحلة الطفولة المتوسطة(Middle childhood) وتبدأ من سن السادسة إل التاسعة أما مرحلة الطفولة المتأخرة (Late childhood) فتبدأ من سن التاسعة إلى سن 12 من عمر الطفل. للمزيد من التفاصيل راجع: النوايسه نانسي خالد سليم، جريمة الاستغلال الجنسي للأطفال عبر الأنترنيت، أطروحة لنيل شهادة الدكتوراه في القانون، كلية القانون، جامعة عمان العربية، الأردن، 2011، ص: 20-21.

[2]- ويكمن الفرق بين مصطلحي" الحدث "و"الطفل"، في كون المصطلح الأول ينصرف للدلالة على قيام المسؤولية الجزائية للطفل من عدمها، أما المصطلح الثاني الطفل يشير إلى كونه محل الحماية الجزائية.

[3]- القانون 15-12 المؤرخ في 2015/07/15 والمتعلق بحماية الطفل، جريدة رسمية عدد 39 لسنة 2015. والذي ألغى أحكام الأمر رقم 72-03 المؤرخ في 25 ذي الحجة عام 1391 الموافق 10 فبراير سنة 1972 والمتعلق بحماية الطفولة والمراهقة، جريدة رسمية عدد 15 لسنة 1972.

أنه كل شخص لم يبلغ سن 18 سنة كاملة، وأضاف تعريفا للطفل في خطر[1] محددا على سبيل المثال بعض الحالات التي تعرض الطفل للخطر ومن بينها: الاستغلال الجنسي للطفل بمختلف أشكاله لاسيما استغلاله في المواد الإباحية وفي البغاء وإشراكه في العروض الإباحية[2].

وعليه طبقا لما تقدم ذكره يمكن القول أن التحرش الالكتروني باعتباره شكلا من أشكال التحرش الجنسي المستحدث والذي يعتبر نتاجا للمستجدات الحديثة التي افرزها الثورة التكنولوجية[3]، ويعرف بأنه كل استعمال لوسائل الكترونية وشبكة المعلومات من أجل التواصل مع القصر وإيذائهم باستخدام رسائل أو صور ذات إيحاءات فاضحة من أجل التغرير بهم واستغلالهم.

ثانيا: أشكال التحرش الالكتروني

لا مجال لإنكار الدور الذي لعبته البيئة الالكترونية في تشجيع سلوكيات التحرش وتوفير الجو لتعزيزها، فعلى الصعيد الوطني وفي تقرير رصدته المصلحة المركزية لمكافحة الإجرام السبيراني التابعة للدرك الوطني، أعلنت معالجة 1140 قضية تتعلق بالجريمة الإلكترونية منذ بداية سنة 2018 إلى غاية 27 من نوفمبر من نفس السنة، 136 قضية منها خاصة بالأطفال وهو رقم في تزايد مستمر مقارنة بالسنة 2017 أين بلغ مجمل قضايا الأطفال 100 قضية تمت معالجتها على مستوى الدرك الوطني[4].

ويتخذ التحرش الالكتروني أو عبر الوسائط الالكترونية عدة أشكال يمكن إجمالها فيما يلي:

---

[1]- عرفت المادة 02 فقرة 04 من القانون 15-12 "الطفل في خطر": الطفل الذي تكون صحته أو أخلاقه أو تربيته أو أمنه في خطر أو عرضة له، أو تكون ظروفه المعيشية أو سلوكه من شأنهما أن يعرضاه للخطر المحتمل أو المضر بمستقبله، أو يكون في بيئة تعرض سلامته البدنية أو النفسية أو التربوية للخطر" .

[2]- أنظر المادة 02 فقرة 14 من القانون 15-12 السالف الذكر.

[3]- رانيا محمود الكيلاني، التحرش الجنسي من الواقع الاجتماعية إلى الفضاء الافتراضي، روابط للنشر وتقنية المعلومات، القاهرة، 2018، ص: 152.

[4]- http://www.aps.dz/ar/sante-science-technologie/63173-1100-2018- visité le 27/01/2020 à 11 :52.

https://www.tsa-algerie.com/ar/%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1-44-%D8%A8%D8%A7%D9%84%D9%85%D8%A7%D8%A6%D8%A9-%D9%85%D9%86-%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1%D9%8A%D9%8A%D9%86-%D9%88%D8%A7%D8%AC%D9%87%D9%88/ visité le 04/02/2020 à 08 :23.

1- بث صور وأفلام ومحادثات منافية للآداب العامة (التحرش البصري)

أو ما يسمى بترويج المعطيات الإباحية التي أصبحت أمرا مألوفا عبر الانترنيت، حيث يتم عرض أو تسجيل أو نقل معطيات منافية للآداب سواء كانت صور أو أفلام فاضحة أو حتى محادثات يهدف الجاني بها التحرش بالقاصر والتأثير عليه لاستماله وحثه على الانحراف والفساد الأخلاقي[1].

وفي هذا الصدد لقد حددت الاتفاقية الأوروبية حول جرائم الانترنت لسنة 2001 المقصود من صور الأطفال الفاضحة على أنها تلك المواد التي توضح بالتصوير المرئي أحد القاصرين مشغولا في ارتكاب فعل أو سلوك جنسي واضح، شخص يبدو أنه قاصر منشغل في ارتكاب فعل أو سلوك جنسي واضح وصور واقعية حقيقية تثبت وجود أحد القاصرين منشغلا في ارتكاب فعل أو سلوك جنسي واضح.

2- التحريض على الفسق (التحرش بالإكراه)

ويقع عن طريق تحايل واستدراج المجرمين لضحاياهم من القصر، بحيث يتم إيهام الضحية برغبة الجاني في تكوين علاقات معه بأسلوب ما تنتهي بالإيقاع بضحيته تتطور مناحيها بعد الاستجابة لمتطلبات المتحرش من محاورات وصور وحتى تسجيل فيديوهات قد تأخذ بعدا فاضحا، ليتم فيما بعد ابتزازه وتهديده بها من خلال الملاحقة الالكترونية أو التشهير عبر المواقع الالكترونية، وفي هذا الشأن صرحت منظمة اليونيسيف في تقرير أصدرته سنة 2009 أن حوالي 750 ألف شخص من مستخدمي الشبكة المعلوماتية يجرون فيها سعيا وراء التواصل بالأطفال والتغرير بهم[2].

وفي هذا السياق، ترجع أول قضية عرفت في هذا الشأن في الولايات المتحدة الأمريكية لطفلة تدعى "أماندا تود" البالغة من العمر 15 سنة، والتي تعرضت للاستغلال والتحرش عبر

---

[1]- سحر فؤاد مجيد، جريمة التحرش الجنسي بالأطفال عبر الانترنيت (دراسة في القانون الأمريكي والعراقي)"، مرجع سابق، ص: 307.

[2]- حسين بن سعيد الغافري، الإطار القانوني لحماية الأطفال من مخاطر شبكة الانترنيت (قراءة في قانون مكافحة جرائم تقنية المعلومات)، ورقة مقدمة لورشة العمل الإقليمية في مجال السياسات وبناء القدرات في مجال حماية الأطفال على الانترنيت، مسقط 30 إلى 31 أكتوبر 2011، ص:05.

الانترنيت بعد استدراجها من قبل أحد الجناة والتغرير بها، وصل لحد التشهير بصورها الفاضحة عبر الانترنيت ما أدخلها في أزمة نفسية انتهت بانتحارها[1].

المحور الثاني: موقف القانون من جريمة التحرش الالكتروني وآليات الردع لمجابهتها

رغم استفحال ظاهرة التحرش الجنسي وظهورها في العديد من دول العالم، من بينها الجزائر التي لم تكن بمعزل عن هذه الظاهرة وعن مثل هذه الممارسات، إلا أن المشرع الجزائري لم يحذو حذو باقي التشريعات المقارنة[2] المجرمة لهذا الفعل إلا في تعديله لقانون العقوبات سنة 2004 وإضافته لنص المادة 341 مكرر منه.

هذا ما سنوضحه من خلال هذا المحور وذلك من خلال بيان الآليات التشريعية الوطنية الموجهة لمكافحة جريمة التحرش الالكتروني بالقصر **(أولا)** ثم التطرق للآليات التشريعية العربية وخصوصا التشريعين الأردني والمصري **(ثانيا)**.

أولا: الآليات التشريعية الوطنية المقررة لمكافحة التحرش الالكتروني بالقصر

في ظل افتقار المشرع الوطني لأية نصوص قانونية تواكب حداثة جريمة التحرش الجنسي وتطور مرتكبيها، تتقيد دراستنا على قانون العقوبات باعتباره النص القانوني الوحيد الذي واجه جريمة التحرش الجنسي وبعض الجرائم الواقعة على القصر ولكن بقواعد تقليدية. بالإضافة إلى قانون حماية الطفل الذي أفرد في بعض نصوصه حماية الكترونية للطفل القاصر يطرح التساؤل حول مدى كفايتها.

1-جريمة التحرش الالكتروني بالقصر في قانون العقوبات المعدل والمتمم

سبقت الإشارة إلى أن أول نص قانوني يجرم فعل التحرش الجنسي كان بموجب تعديل 2014، حيث نصت المادة 341 مكرر في فقرتها الأولى من قانون العقوبات على أنه: "يعد مرتكبا لجريمة التحرش الجنسي ويعاقب بالحبس من شهرين (2) إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل شخص يستغل سلطة وظيفته أو مهنته عن طريق إصدار الأوامر للغير أو بالتهديد أو الإكراه أو بممارسة ضغوط عليه قصد إجباره على الاستجابة لرغباته الجنسية".

---

[1]- https://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd, visité le 19/02/2020 à 18:30.

[2]- جدير بالإشارة أن المشرع الفرنسي يعد أول من تناول جريمة التحرش الجنسي في تشريعه من بين الدول الأوروبية وهذا بموجب المادة 1/3/220 من قانون العقوبات لسنة 1992. نقلا عن : بن أعراب محمد، "التحرش الجنسي في الجزائر من الطابوهات المسكوت عنها إلى التجريم القانوني"، مجلة الآداب والعلوم الاجتماعية، جامعة فرحات عباس، سطيف، بدون عدد أو سنة، ص: 451.

يتضح من خلال هذا النص أنه جاء بعمومية تامة، فيؤخذ عليه أنه تناول التحرش الجنسي كجريمة تقليدية فلم يتطرق للطابع الافتراضي للجريمة، فكان عليه التوسع أكثر في أشكال التحرش كما لو نص على أنه: "يعد مرتكبا لجريمة التحرش الجنسي **كل من تسبب في مضايقة للغير أفعالا أو أقوالا في مكان عمومي أو عن طريق وسائل الاتصال السلكية واللاسلكية**". ومن جهة أخرى الملاحظ أن نص المادة قد حصر المتحرش في الشخص صاحب السلطة فقط وهو ما يتضح من عبارة "**كل شخص يستغل سلطة وظيفته أو مهنته...**" ما يجعل النص مواكبا أكثر للتطبيق على الأشخاص المتحرش بهم في أماكن العمل.

وبالتالي يمكن القول أن المشرع الجزائري قد تبنى النظرية القائلة بأن أساس الجريمة لا يتغير ولو ارتكب عن طريق الشبكة المعلوماتية، وبالتالي لا مجال إلا لتطبيق تلك النصوص الواردة في قانون العقوبات تحت محتوى الاعتداء وهتك العرض و انتهاك الآداب العامة. وفي هذا الشأن تنص المادة 330 مكرر01 من قانون العقوبات والمضافة بموجب تعديل 14-01 والتي جرمت كل من التقط صورا لقاصر **بأي وسيلة كانت** وهو يمارس أنشطة جنسية أو صورا لأعضائه أو أنتج أو وزع أو نشر أو روج أو استورد أو صدر أو عرض أو باع أو حاز مواد إباحية لقاصر بعقوبة من 05 سنوات إلى 10 سنوات وبغرامة من 500.000 إلى 1000.000 دج.

كما تضيف المادة 342 في فقرتها الأولى من نفس القانون على تجريم فعل تحريض القاصر على الفسق الدعارة فنصت على أنه: "كل من حرض قاصرا لم يكمل 18 سنة كاملة على الفسق أو فساد الأخلاق أو تشجيعه عليه أو تسهيله له ولو بصفة عرضية، يعاقب بالحبس من 05 سنوات إلى 10 سنوات وبغرامة من 20.000 دج إلى 100.000 دج".

2-جريمة التحرش الالكتروني بالقصر في قانون حماية الطفل 15-12

لقد أفرد قانون حماية الطفل بعض الحماية القانونية للقاصر المتحرش به الكترونيا، فتضمنت نصوصه على بعض القواعد القانونية بعيدا عن قانون العقوبات، في المادتين 140 و141 منه وأحال الباقي لقانون العقوبات.

وتضمنت المادة 140 منه: "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 150.000دج إلى 300.000دج ، كل من ينال أو يحاول النيل من الحياة الخاصة للطفل بنشر أو ببث نصوص و/أو صور بأية وسيلة يكون من شأنها الإضرار بالطفل"

كما أضافت المادة 141 تجريم استغلال الطفل عبر وسائل الاتصال أيا كان شكلها في سلوكات منافية للآداب العامة والنظام العام، حيث جاء فيها: "دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 150،000دج إلى 300،000دج، كل من يستغل الطفل عبر وسائل الاتصال مهما كان شكلها في مسائل منافية للآداب العامة والنظام العام."

ليكون بذلك أول نص في التشريع الوطني يعترف بالطابع الافتراضي لجريمة استغلال الطفل والتحرش به، كأن يستدرج الجاني أحد القصر عبر مواقع التواصل الاجتماعي ويوهمه بإقامة علاقة صداقة معه ويقنعه بعد ذلك على تنفيذ أعمال إباحية له سواء بإرسال صور فاضحة له أو عن طريق محاكاة مباشرة عبر الفيديو سواء بعوض أو بدون عوض.

وهو ما حدث في قضية أفرزتها مصالح الدرك الوطني في مارس 2017 أين أوقعت بشخص بالغ 27 سنة معالج خطاب والمدعو ف.ب، الذي يتتبع الأحداث الصغار على الشبكات الاجتماعية. ووفقا للبيان الصحفي الصادر عن الدرك الوطني، فإن لدى الأخير حوالي 8 حسابات على *Facebook*، 3 منها تم تحديدها على أنها حسابات للفتيات الصغيرات من أجل الإيقاع بضحاياه الذين لم تتجاوز أعمارهم 14 عامًا. كان الهدف هو التقاط صور لهم في مواقف غير لائقة ومضايقتهم بعد ذلك إذا لم تستجب الضحية لاستغلاله[1].

ثانيا: الآليات التشريعية العربية المقررة لمكافحة جريمة التحرش الالكتروني بالقصر

نحو انتهاج سياسة عقابية لمكافحة جريمة التحرش الالكتروني بالقصر، أفرزت بعض التشريعات العربية اجتهادا كبيرا في إرساء الحماية القانونية للمتحرش بهم لاسيما تلك الأفعال الممارسة على القصر عن طريق شبكة الإعلام والاتصال.

1-التشريع الأردني

إدراكا منه بخطورة الجريمة المعلوماتية عامة وتلك الماسة بفئة الأطفال القصر خاصة، تجاوز المشرع الأردني القصور في توفير الحماية اللازمة للقاصر في الجرائم الالكترونية بنصوص قانونية تتناسب وحداثة الجريمة وتطور مرتكبيها وتقنيتهم. وهذا من خلال إصدار قانون الجرائم الالكترونية رقم 27 لسنة 2015 حيث تضمنت المادة 09 منه في فقرتيها (أ) و(ب) تجريما لكل من استخدم الشبكة المعلوماتية ضد الأطفال لاستغلاله والتحرش به أو تحريضه على

[1] -https://www.elwatan.com/edition/actualite/crimes-electroniques-les-mineurs-comme-cible-05-04-2017 visité le 11/01/2020 à 21 :11.

الانحراف. وجاء فيها: " أ. يعاقب كل من أرسل أو نشر عن طريق نظام المعلومات أو الشبكة المعلوماتية قصدا كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالا إباحية أو تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر بالحبس مدة لا تقل عن 03 أشهر ولا تزيد عن سنة وبغرامة لا تقل عن 300 دينار ولا تزيد عن 5000 دينار.

ب. يعاقب كل من قام قصدا باستخدام نظام المعلومات أو الشبكة المعلوماتية في إنشاء أو حفظ أو إعداد أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل 18 سنة من العمر أو من هو معوق نفسيا أو عقليا، أو توجيهه أو تحريضه على ارتكاب جريمة، بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 1000 دينار ولا تزيد عن 5000 دينار".

من هذا النص يتضح أن تجريم المشرع الأردني للأعمال الإباحية لم يكن عاما وإنما اقتصر على فئة الأطفال والأشخاص المعوقين نفسيا أو حركيا، كون هذه الأفعال الموجهة ضدهم أكثر خطورة وأدق تأثيرا لديهم لعدم وعيهم واندفاعهم يسهل التأثير والتغرير بهم.

2-التشريع المصري

ويعتبر من أهم التشريعات العربية التي بادرت بتوفير الحماية القانونية للطفل، حيث كانت جمهورية مصر العربية من أول عشرين دولة صدقت على اتفاقية حقوق الطفل "الاتفاقية" سنة 2001، ولم يعد لديها أية تحفظات عليها، كما صدقت على كل الوثائق الدولية والإقليمية المعنية بحماية الأطفال[1]. وترجمت المبادئ الدولية المستقر عليها والمتبناة في تشريعاتها الوطنية فسنت القانون رقم 12 لسنة 1996 بشأن الطفل.

ومع تطور الشبكة المعلوماتية وتزايد الجرائم الالكترونية المرتكبة ضد القصر لاسيما التحرش بهم واستغلالهم جنسيا، تحرك المشرع المصري لإدخال تعديلات على قانون الطفل حتى تكون نصوصه أكثر مواكبة مع حداثة الجرائم وهذا بموجب القانون رقم 128 لسنة 2008.

حيث جرم المشرع المصري من خلال المادة 116 مكرر أ من قانون الطفل المصري الأفعال الخاصة بإنتاج أو اقتناء أو توزيع أو طبع أو حيازة أو بث أعمال إباحية يشارك فيها

[1]- تقرير جمهورية مصر العربية حول التدابير التي اتخذتها لتنفيذ أحكام البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلالهم في البغاء وفي المواد الإباحية المقدم إلى لجنة الأمم المتحدة لحقوق الأطفال عن الفترة 2004-2009، يناير 2010 منشور عبر موقع: https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.OPSC.EGY.1_ar.doc.

الأطفال أو تتعلق بالاستغلال الجنسي، فأقر عقوبة الحبس لمدة لا تقل عن السنتين وبغرامة مالية حددت قيمتها الأدنى بـ 10.000 جنيه وقيمة قصوى لا تتجاوز 50.000 جنيه.

لتضيف ذات المادة اقتران هذه الأفعال باستعمال شبكة الانترنيت فجاء فيها: "مع عدم الإخلال بأي عقوبة أشد ينص عليها قانون آخر يعاقب بذات العقوبة كل من:

1-استخدم الحاسب الآلي أو الانترنيت أو شبكة المعلومات أو الرسوم المتحركة لإعداد أو حفظ أو لمعالجة أو لعرض أو لطباعة أو لنشر أو لترويج أنشطة أو أعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة أو الأعمال الإباحية أو التشهير بهم أو بيعهم.

2-استخدم الحاسب الآلي أو الانترنيت أو شبكة المعلومات أو الرسوم المتحركة لتحريض الأطفال على الانحراف أو لتسخيرهم لارتكاب الجريمة أو على القيام بأنشطة أو أعمال غير مشروعة أو منافية للآداب ولو لم تقع الجريمة فعلا ".

والواضح من هذا النص أن المشرع المصري قد خرج عن نطاق تطبيق النصوص التقليدية على جريمة التحرش الالكتروني بالقاصر بإفراد نصوص قانونية أكثر حداثة تواكب الجريمة وتطور مرتكبيها.

خاتمة:

مما سبق خلصت الدراسة إلى ما يلي:

- تعتبر الجرائم المعلوماتية أحدث الجرائم التي ساهمت في توسعها الانفتاح على شبكة الانترنيت، ما يميزها على الجرائم التقليدية والتي باتت تشغل اهتمام العديد من التشريعات لاسيما في ظل تطور هذه الجريمة وتوسع نشاط مرتكبيها عبر مواقع الانترنيت.
- تعتبر جريمة التحرش الالكتروني بالقصر أحد صور الجرائم المعلوماتية وأبشعها، التي تستخدم فيها الوسائل الالكترونية وشبكة الانترنيت في تتبع الضحايا وإزعاجهم بإيماءات أو رسائل ذات طابع جنسي، تؤثر سلبا على بناء شخصياتهم وسلوكياتهم.
- إن جريمة التحرش الالكتروني ما هي إلى امتداد لجريمة التحرش الجنسي المنصوص عليها في قانون العقوبات والتي ترتكب بوسائل مستحدثة للمساس بحياة القصر وحرمته، خرجت بالجريمة من الواقع الاجتماعي إلى الفضاء المعلوماتي ما يستلزم وجود آليات تشريعية تضمن حماية للطفل.

- تمايزت مواجهة التشريعات لجريمة التحرش الالكتروني بين نصوص مستحدثة ونصوص تقليدية، ومقارنة بالتشريعات العربية محل الدراسة الملاحظ قصور المشرع الجزائري عن مجابهة

جريمة التحرش الالكتروني بالقصر بحيث اكتفى بالنصوص العقابية التقليدية التي لم تعد تواكب حداثة الجريمة وتطور الجناة ما يجعل موائمة النصوص التقليدية للجريمة المستحدثة أمرا صعبا.

صور الجريمة المعلوماتية في ظل التشريع المغربي والمصري

Information crime in light of Moroccan and Egyptian legislation

د. شيماء الهواري
جامعة الحسن الثاني الدار البيضاء المملكة المغربية.

المقدمة

أدى الانتشار الكبير لاستعمال وسائل التواصل و الانترنت بين أفراد المجتمع إلى ظهور صنف اجرامي جديد، يطلق عليه الجرائم الإلكترونية، كالنصب والاحتيال الإلكتروني و المعلوماتي...، ومن بين أشكال هذه الظاهرة الإجرامية: تفشي التنمر والابتزاز الإلكتروني.... هذه الظواهر يعود سببها إلى الازدياد المهول في وتيرة التطور التقني للمعلوماتية، واتساع استخدام وسائل التواصل الحديثة، وانعكاسها على مختلف أشكال المعرفة الإنسانية، وتغييرها نمط حياة الأفراد، وأيضا على قيم المجتمعات . ويعد التنمر بجميع صوره؛ سواء كان مضايقة الضحية، تشويه سمعتها، انتقادها، انتحال هويتها، أو خداعها والاحتيال عليها...، إضافة إلى الابتزاز الإلكتروني، من أخطر صور الجرائم الإلكترونية، نظرا إلى آثارها السلبية على نفسية الشخص، والتي قد تؤدي به إلى الدخول في اكتئاب حاد قد يوصله إلى حد الانتحار.

كما بدأت تطفوا على السطح ظاهرة اختراق الحسابات الشخصية على مواقع التواصل الاجتماعي وسرقت محتوياتها الشخصية؛ كالصور او نشر فيديوهات إباحية او سرقت معلومات مالية لشركات او أفراد؛ كرقم بطاقة الائتمان البنكي وغيرها.

هذا التلاعب الإلكتروني الذي يقوم به أفراد في غاية البراعة في ميدان تكنولوجيا المعلومات، والذي نجد ان غالبيتهم لا سوابق عدلية لهم وحتى أن اغلبهم قاصرين، وضع المشرع القانوني في الزاوية الضيقة حيث أن غالبية الدول لم تكن قد أوجدت قوانين تحمي رواض العالم الافتراضي، لكن بعد تفشي هذا الصنف الإجرامي استوجب على فارض القانون أن يضع مجموعة من النصوص القانونية التي تجرمهم وتفرض عقوبات عليهم بين الحبس وبين الغرامات المالية.

هذه الجرائم قد تؤدي بالضحية إلى محاولات الانتحار، وفي حالات أخرى إلى الرضوخ لمطالب المجرم التي تكون غالبا مستفزة وغير إنسانية.

في جمهورية ككوريا الجنوبية معدلات الانتحار مرتفعة بين المراهقين والشباب والسب بنسبة كبير يرجع إلى الابتزاز الإلكتروني والتنمر على مواقع التواصل الاجتماعي. كما أكدت بعض التقارير

الصحفية ان من كان ينجوا من الانتحار او التشهير يصبح ضحية للقرصان الالكتروني ومستعبدا لديه، حيث يتم استغلال الضحية في أعمال غير مشروعة وخاصة الأفلام الإباحية، او الانتساب لشبكات الدعارة الدولية للقاصرين او الاتجار بالمخدرات ناهيك عن عصابات النصب والاحتيال.
وتحاول السلطات الكورية الجنوبية و سلطات دولة الفلبين وفي أوروبا ايضا وخاصة الشرقية إضافة إلى هولندا محاربة هذه الآفة بشتى السبل عبر النشرات الإعلانية على مواقع الإباحية ومواقع التسوق الإلكترونية، وأيضا على صفحات الجامعات الالكترونية...إضافة إلى حملات اشهارية تضامنية مع كل ضحايا التنمر والابتزاز عبر تكرار كلمات ك: لست وحدك .
في خضم هذا التطور المخيف في عالم الجريمة، قام المشرع المغربي والمصري بتجريم هذه الأفعال، وخصص لها المشرع المصري قانونا فرد لها وهو "قانون جرائم تقنية المعلومات المصري"، أما في المغرب فمازال المشرع يعتمد على القانون الجنائي في معالجة مثل هذه القضايا، غير انه يتم تداول مشروع قانون تحت قبة البرلمان المغربي يهدف إلى تجريم بعض الأفعال على مواقع التواصل الاجتماعي والانترنت وهو ما سمي بقانون تكميم الأفواه او قانون 20-22 .
وللتعرف أكثر على القوانين المخصصة لمواجهة الجريمة المعلوماتية في مصر والمغرب، سنعمل على تقديم وتحليل مواد وفصول كل قانون على حدى، وتبيان العقوبات والغرامات المفروضة في كل منها، مع تقديم توصيات مناسبة لتطوير القوانين .

عناصر المقدمة :

الإشكالية العامة: هل المشرع المغربي والمصري قام بالتنصيص على مواد وبنود قانونية للحد من الجريمة الإلكترونية المعلوماتي المتجددة ام ان المشرع العربي يستغلها لتحقيق مأرب سياسية اكثر من حماية الفرد .

إشكاليات البحث : الجريمة المعلوماتية او الإلكترونية هي صنف إجرامي متطور بذاته يخضع للتطور السريع في مجال تكنولوجيا المعلومات. هذا الصنف الإجرامي يؤثر بشكل كبير على الحياة الخاصة للأفراد والجماعات والمؤسسات السياسية والاقتصادية و حتى الدول. ولتجريمه يجب أن تكون القوانين سريعة التجدد وتواكب التطور العلمي في مجال المعلوماتية.
إذن ما هي الجريمة المعلوماتية او جرائم الالكترونية او جريمة تقنية المعلومات؟ ما هي العقوبات الرادعة لها؟ وكيف يصنفها المشرع المغربي والمصري؟ وهل القوانين الحالية تحد من مثل هذه الجرائم؟ مجموعة من التساؤلات تستوجب الرد عليها، وهذا ما سنعمل عليه في هذه الدراسة.

تأليف مجموعة من الباحثين

أهداف الدراسة : تهدف الدراسة إلى تحليل مواد ونصوص كل من قانون مكافحة الجريمة المعلوماتية المصري والمغربي، وخلق فرصة لوضع أيدينا على مكامن الخلل فيهما.

خطة الدراسة: تقتضي هذه الدراسة البحث في تعريف الجريمة الالكترونية او المعلوماتية وأنواعها، والعقوبات القانونية في كل من القانون المصري والمغربي، ناهيك عن صور الجريمة المعلوماتية في التشريع المصري والمغربي، كما سنعمل على وضع توصيات لتطوير هذه القوانين .

المطلب الأول: الجريمة المعلوماتية في التشريعين المغربي و المصري

بعد الحراك العربي وما نتج عنه من توابع سياسية واقتصادية وعمد المشرع العربي الى تعديل وخلق مجموعة من القوانين تناسب الوضع السياسي لبعض الدول العربية، هذه القوانين كانت تهم تعديلات في الدساتير وأيضا في قوانين الانتخابات الرئاسية و البرلمانية، لكن اهم ما شمله التعديل هو تعديل وخلق قوانين تقيد وتنظم في ان واحد المجال الاعلامي الالكتروني سواء مجال الصحافة الالكترونية وايضا الحياة العامة والفردية على صفحات الانترنت .

الفرع الأول: الجريمة المعلوماتية في القوانين المغربية

عالم الجريمة المعلوماتية يعتبر من العوالم الصعبة التحكم و السيطرة، لذلك عمد المشرع المغربي الى تطويق هذا المجال بمجموعة من النصوص القانونية المهمة .

الفقرة الاولى :طبيعة الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية فعلا جرميا يهدف بالأساس إلى الإضرار بمصالح الآخرين من خلال وسائل متعددة ومتنوعة وفقا لكل حالة ولكل هدف مراد الاضرار به، وهو ما يجعلها لا تختلف عن الجرائم التقليدية في نتيجتها الاجرامية، وبوصفها فعلا جرميا كأي جريمة أخرى، فإنه لابد أن يتوافر في ذلك الفعل مجموعة من الشروط والأركان الواجب تحققها وذلك بهدف التأكد من وقوع الفعل الجرمي وفق ما يقرره القانون، وتحديد آلية العقاب والإدانة فيما بعد.

وكسائر الجرائم الأخرى، فإنها تتوافر على مجموعة من الخصائص والأنواع تميزها في كثير من الحالات عن الجرائم التقليدية الأخرى.

وتأسيسا على ذلك: سنقوم بتقسيم المبحث إلى مطلبين، أولهما يتناول تعريف الجريمة المعلوماتية وأنماطها، وفي المطلب الثاني سيتم تناول الجوانب المتعلقة بأركان الجريمة المعلوماتية وأنماطها

أ. ماهية الجرائم المعلوماتية:

للجريمة المعلوماتية العديد من التعريفات في أوساط الفقه الجنائي وذلك يرجع باعتبارها فعلا مستحدثا من جهة، وتختلف في الشكل والتركيب حسب نوع الفعل المرتكب من جهة أخرى.

ب.الجريمة المعلوماتية:

عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الجريمة المعلوماتية بأنها " كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب"

إن كثرة التوجهات والآراء لم تساعد على وضع تعريف محدد وشامل للجريمة المعلوماتية، وهو ما يدفع عموما إلى وصفها بأنها ذلك " النشاط الإجرامي الذي يكون النظام المعلوماتي أو الشبكة المعلوماتية جزء جوهري في الجريمة أو أن تكون التكنولوجيا في حد ذاتها الهدف"، أو " بأنها ذلك النشاط الإجرامي الذي يعتبر الحواسيب أو الشبكات المستخدمة من أجل تحقيق نتيجة إجرامية"

وعليه يمكننا تعريف الجريمة المعلوماتية بأنها " الفعل المجرم قانونا سواء بامتناع أو إتيان بأفعال من شأنها الإضرار بمصالح الآخرين سواء تعلقت بالجوانب المالية أو الشخصية أو الأدبية باستعمال وسائل أو أدوات تكنولوجية حديثة عبر الفضاء الافتراضي."

الفقرة الثانية : أنماط الجريمة المعلوماتية

تختلف أنماط الجرائم المعلوماتية حسب النوع والهدف من ارتكابها وذلك بغية تحقيق أكبر ضرر ممكن عبر استخدام كافة الوسائل الإلكترونية الممكنة، وتتنوع ما بين ذات الطابع السياسي والعسكري والأفراد والشبكات المعلوماتية، وهو ما يعطيها تكيفات مختلفة.

في الجرائم المعلوماتية يحدد نمط الجريمة بمدى تعلق الجريمة بالحاسوب، فقد يعتبر في إحدى الحالات هو العنصر الرئيسي في تنفيذها أو يتضاءل ويلعب فقط دورا ثانويا، وقد لا تقوم من الأساس بدون حاسوب، وقد يكون الحاسوب نفسه هو محل النشاط الإجرامي.

أ: الجرائم المعتمدة على الحاسوب في التنفيذ

الحاسوب في هذه النقطة يكون هو الأداة الرئيسية لارتكاب الجريمة وذلك لما يحتويه من معلومات وأصول، وبالتالي لا يمكن اعتباره فقط وسيلة ارتكاب الجريمة أو مضاعفتها، بل إنه يتحول إلى الباعث في ارتكاب الجريمة (حالة التحويل غير المشروع للأرصدة البنكية)، وكذلك في حال استخدامه لتزوير الأوراق المالية وهو ما قررته استئنافية البيضاء في قرار لها بقولها " إن إقدام المتهمة على صنع أوراق نقدية بطريقة السكانير لها مظهر الأوراق الحقيقية وتسليمها للمتهمين قصد التداول يظهر نيتها الجرمية ويجعل أفعالها تطالها مقتضيات الفصل 334 من ق.ج

ب: الجرائم التي يؤدي الحاسوب فيها دورا ثانويا

وتكون الجريمة في هذه الحالة قابلة للتنفيذ بأدوات ووسائل أكثر أهمية من الحاسوب والذي يتحول لمجرد عامل ثانوي كمجرد وسيلة لإتمام الجريمة (حالة استعمال آلات متخصصة لقرصنة المعلومات البنكية والمالية من بطائق الائتمان وربطها بالحاسوب فيظهر عدد العمليات المسجلة ويتم نقلها لاستغلالها في تصنيع بطائق بنكية مزورة)

ت: الجرائم المرتبطة وجودها بالحاسوب

وجود الحاسوب وأنظمته يعتبر شيئا ضروريا لارتكاب مثل هذه الجرائم، حيث ترتكب في مواجهة ومساعدة الحاسوب والاستعمال غير المصرح بها للحاسب الآلي أو الاستعمال غير المشروع لبرامجه.

ث: الجرائم التي يكون الحاسوب في فيها محلا للنشاط الإجرامي

وقد يتغير وضع الحاسوب في هذه الحالة من الوسيلة إلى الهدف المطلوب إصابته، من خلال تركيز أفعال التخريب والإتلاف عليه ومهاجمة محتوياته الأساسية قصد تعطيبها أو إتلافها نهائيا (كالفيروسات الإلكترونية التي يكون الهدف منها إصابة الأقراص الصلبة للحواسيب)

الفقرة الثالثة : تكييف وأركان الجرائم المعلوماتية

فالجرائم بطبيعة الحال تختلف باختلاف الواقعة القانونية المرتبطة بها فهي تتحقق بمجرد استكمالها للأركان الأساسية.

أ- تكييف الجريمة المعلوماتية

فالجريمة المعلوماتية قد تكون إما جرائم واقعة على الأموال، أو جرائم واقعة على الأشخاص، أو جرائم واقعة على أمن الدولة

- **الجرائم الواقعة على الأموال:**

مع تحول معظم المعاملات التجارية كالبيع والشراء قصد تسهيلها إلى استخدام وسائل الدفع والوفاء الالكترونية عبر شبكة الانترنيت، ظهرت عمليات السطو الالكتروني والتحويل الالكتروني غير المشروع للأموال بالإضافة على قرصنة البطاقات الممغنطة.

- **جريمة السطو على أرقام بطائق الائتمان والتحويل الالكتروني غير المشروع للأموال**

من خلال استخدام البطائق في المعاملات المشار إليها أنفا، فإن الجناة في الجريمة المعلوماتية يعملون على السطو عبر استخدام الوسائل الالكترونية المتاحة من خلال سرقة الأرقام الخاصة بتلك البطاقات وبيعها لاحقا عبر الانترنيت لأطراف أخرى بالاستعانة بالاحتيال الرقمي من خلال ايهام المجني عليهم بوجود مشروع مربح يكون في الحقيقة عمل وهمي، يوتم من خلاله

التحويل المالي باستخدام الانترنيت أو من خلال تصرف الجاني في المال بدون توافره على تلك الصفقة وهذه الحالة تجعل من الجريمة أقرب إلى جريمة النصب من الجرائم الماسة بنظم المعطيات وهو ما ذهبت إليه المحكمة الابتدائية بالرباط بقولها " ذلك أنه فضلا عن انكار الظنين لهذه الواقعة فإن المراسلات عبر البريد الالكتروني لا تدخل ضمن المعالجة الآلية التي يحميها الفصل 607 من القانون الجنائي، الشيء الذي اقتنعت معه المحكمة بعدم ارتكاب المتهم للجنحتين المذكورتين مما يتعين القول في حقه بحكم الأصل والتصريح ببراءته منهما" ، أو باتخاذ الولوج مباشرة لبيانات الحواسيب المتعلقة بالمجني عليهم

- **القمار وغسيل الأموال عبر الانترنيت**

توجد العديد من الجهات المتخصصة في ممارسة ألعاب القمار على شبكة الإنترنيت، وذلك بإضفاء قدر كبير من الخصوصية وإخفاء شخصيات اللاعبين، وتتداخل هنا عمليات غسيل الأموال مع ممارسة القمار عبر الأنترنيت وذلك بما تقدمه شبكة الانترنيت من تسهيلات بالإضافة إلى سرعتها وعدم وجود حدود جغرافية، وهو ما جعل من المواقع الافتراضية لممارسة القمار دائما ما تكون محل اشتباه ومراقبة مستمرة من قبل الشرطة الفنية وجهات محاربة غسيل الأموال

➢ **الجرائم الواقعة على الأشخاص:**

فمن بين الجرائم الواقعة على الأشخاص نجد جريمة التهديد والمضايقة والملاحقة، جريمة انتحال الشخصية والتغرير بالغير، جرائم السب والقذف، ثم لا ننسى المستحدث التشريعي فيما يعرف بجرائم التشهير بالأشخاص.

- **جريمة انتحال الشخصية والتغرير بالغير**

تتم هذه الجريمة من خلال استخدام البريد الالكتروني بإرسال رسائل تحمل في فحواها التهديد والابتزاز للمجني عليه بارتكاب جريمة ضده وتستخدم وسائل متعددة إلى جانب البريد الالكتروني فيها كالتطبيقات وبرامج المحادثة المنتشرة على الانترنيت، ولا تتطلب تلك الجريمة اتصال مادي بين الجاني والمجني عليه وذلك لقدرة الجاني على إخفاء هويته والتمادي في ارتكاب الجريمة.

- **جريمة انتحال الشخصية والتغرير بالغير**

وقصد بهذا النوع من الجرائم قيام الجاني بادعاء شخصية غير شخصيته الحقيقية وذلك للاستفادة من سمعته أو ماله أو صلاحياته، وكذلك محاولة التغرير بالغير -خاصة - حينما تحدث عن القاصرين من مستخدمي الانترنيت وذلك من خلال إعطائهم صورة وهمية برغبتهم تكوين صداقات عبر الانترنيت والسعي نحو تطويرها وذلك قصد تحقيق هدف إجرامي معين

- جرائم السب والقذف

تعد جرائم السب والقذف من أكثر الجرائم شيوعا في نطاق شبكة الأنترنيت، وباعتباره وسيلة من وسائل الاتصالات السمعية والبصرية كما هو الحال مع الإذاعات والقنوات التلفزيونية والصحف والمجلات، فقد تتم جريمة السب والقذف عير أي وسيلة من الوسائل السابقة، وقد ذهبت المحكمة الابتدائية بالرباط إلى القول ب " وحيث إن وسائل الاتصال بما فيها المكتوبة يمكن أن تستخدم من أجل الخير وهذا هو المطلوب لكن يمكن كذلك أن تكرس لأغراض الشر والذي يتحمل في النهاية تصحيح المسار والحد من الانزلاقات هو جهاز القضاء... وحيث إنه استنادا لما ذكر أعلاه اقتنعت المحكمة بثبوت جنحة القذف بكافة أركانها المادي بجميع عناصره من فعل الاسناد وموضوع الإسناد والمسند إليه وركن العلنية بالنشر بالجريدة الرسمية طبقا للفصل 38 من قانون الصحافة والنشر وأخيرا القصد الجنائي وبالتالي يتعين مؤاخذة الضنين الأول من أجلها"

➢ الجرائم الواقعة على أمن الدول

وهي الجرائم التي يكون القصد منها الإضرار والمساس بأمن الدول بشكل خاص، وتتنوع تلك الجرائم بين جرائم الإرهاب من خلال المواقع التي تمثل تلك الجماعات الإرهابية وتعمل على شن حرب نفسية ضد الدول والشعوب وتعمل كذلك على الترويج لنفسها، ونشر أخبار ومعلومات تضليلية

ومع سهولة تجميع المعلومات وتخزينها، فإن تلك الملومات وحتى إن توافرت لها نظم حماية معلوماتية قوية تكون عرضة للاختراق والتجسس عليها وذلك قصد الاطلاع عليها والحصول على الأسرار التي بها، ولذلك فإن عملية التجسس على المنظمات والدول ومؤسساتهما تكون أكثر سهولة مالم يتم اتخاذ أكبر قدر من الحيطة والتجديد على مستوى العمل الوقائي للشبكات والأنظمة المعلوماتية الداخلية.

ب: أركان الجريمة المعلوماتية

فالجريمة بطبيعة الحال لتقوم لابد من توفر الشرط المفترض أي ما يعرف بالأساس القانوني الزجري، والركن المادي، ثم الركن المعنوي.

➢ الركن القانوني للجريمة

يعرف أيضا بالركن الشرعي، ومؤداه أن أي تصرف صادر من الفرد لا يكتسب صفة الجريمة، إلا إذا خضع لنص يجرمه ويعاقب عليه القانون الجنائي، حتى ولو أضر بالغير، شريطة ألا يخضع في ظروف ارتكابه لسبب من أسباب التبرير أو الإباحة.

وهذا المبدأ مشهور أيضاً وهو المعبر عنه بمبدأ شرعية التجريم والعقاب، أو ما يصطلح عليه في المجال القانوني بمبدأ " لا جريمة ولا عقوبة إلا بنص"

وقد نال هذا المبدأ اهتماما بالغا جعله يكتسب صفة العالمية، بحيث تأكد عليه جل إن لم نقل كل التشريعات الجنائية الحديثة، ونظرا لما يكتسيه -هذا المبدأ- من قيمة تشريعية، فبالنسبة للمغرب فقد تصدر قمة الهرم التشريعي، حيث ينص الدستور المغربي لسنة 2011 على غرار الدساتير السابقة، على أنه " لا يلقى القبض على أحد ولا يعتقل ولا يعاقب إلا في الأحوال وحسب الإجراءات المنصوص عليها في القانون"

هذا إلى جانب أنه تم تكريس هذا المبدأ عبر مجموعة من المواثيق الدولية والإعلانات العالمية، لعل من أبرزها الإعلان العالمي لحقوق الإنسان لسنة 1948.

كما لا يفوتنا بالتنبيه والتأكيد إلى شريعتنا الإسلامية كان لها السبق في التأكيد على هذا المبدأ، قبل انتشاره في القوانين الجنائية الأوربية وخاصة إيطاليا، التي استوحته من القوانين التي استحدثتها الإمبراطورية العثمانية اعتمادا على مبادئ الشريعة الإسلامية.

- **الركن المادي**

يتمثل الركن المادي في الجرائم المعلوماتية بالدخول غير المشروع إلى نظم وقواعد معالجة البيانات، وذلك دون اشتراط إلى وجود تلاعب بهذه البيانات من عدمه، وذلك لأن مجرد الدخول بأي شكل أو وسيلة غير مشروعة للمواقع المعلوماتية أو الأنظمة الحاسوبية يجعل من النشاط الإجرامي في هذه الحالة متحققا، وقد نص المشرع المغربي في الفصل 3-607 من القانون الجنائي " يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2.000 إلى 10.000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات عن طريق الاحتيال."

ويعاقب بنفس العقوبة من بقي في نظام المعالجة الآلية للمعطيات أو جزء منه، كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله، وتضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو اضطراب في سيره."

ويتمثل السلوك الإجرامي في الجريمة المعلوماتية في ارتباط المعلومة الموجودة على الأجهزة الحاسوبية أو النظام المعلوماتي، والسلوك الإجرامي ليس بحاجة إلى تلك الإجراءات الكثيرة لارتكاب الجريمة، فقد يتحقق بمجرد ضغطة زر على وسيلة تنفيذ الجريمة فيتم تدمير النظام المعلوماتي أو إحداث التزوير أو السرقة عن طريق التسلل إلى أرصدة البنوك والاستيلاء على ما فيها والنسخ والتقليد وانتهاك حقوق المؤلف بحيث تعتبر هذه التجاوزات المادية وسيلة لإثبات س.ج

وبخصوص النتيجة الإجرامية، فمدى تحققها في العالم الإفتراضي أو امتدادها للعالم المادي، ومدى اقتصارها على مكان واحد أم امتدادها لتشمل دول وأقاليم أخرى

وبخصوص الرابطة السببية، فمع التعقيدات المرتبطة بمجال الحاسوب والتقنيات وتطوره بشكل مطرد، بالإضافة إلى التجديد المستمر في أساليب الاتصال بين الأجهزة المعلوماتية وتعدد مراحلها التي تمر بها كذلك، فإن الأوامر المدخلة والخارجية في مراحل التنفيذ، تجعل عملية تحديد السب أو الأسباب الحقيقية للفعل الجرمي المرتكب شيئا صعبا للغاية.

وتتعدد مظاهر الركن المادي للجريمة المعلوماتية وذلك حسب نوعها، فمثلا قد يتمثل الأخير في إدخال بيانات غير معروفة للحاسوب المراد الإضرار به، أو الاتلاف والحذف من خلال عمليات التخريب والمسح الكامل للمعلومات، أو التزوير وتغيير الحقيقة واستعمال الوثائق المزورة، أو تعطيل مفاتيح التشفير وفك رموز الإشارات والاعتداء على نظام الحقوق والمصنفات

- **الركن المعنوي**

يتحقق الركن المعنوي في الجرائم المعلوماتية في علم الجاني أنه يرتكب عبر شبكة الانترنيت أفعال كجريمة على الصعيد القانوني واتجاه ارادته لارتكاب ذلك الفعل أي لابد من توافر "إرادة آثمة" لديه مع توجيهها نحو القيام بعمل غير مشروع قانونا، بالإضافة إلى أهمية توفر نتيجة إجرامية ناتجة عن الأفعال السابقة فتكتسب إرادة الجاني طابع التجريم من الفعل الجرمي المرتكب النابع عن ارتكابها مع توافر علمه بالآثار المترتبة عنه كما هو الحال في جريمة تقليد المصنفات والبرامج الحاسوبية وعرض المنتجات الأدبية والفكرية بدون إذن صاحبها على شبكة الأنترنيت دون إذن مؤلفيها وذلك بتوجه علم الجاني وإرادته نحو ذلك[1] .

الفقرة الرابعة : الحماية القانونية من الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات

---

[1] - القانون الجنائي المغربي

من خلال التطور الذي عرفته الجريمة المعلوماتية وفي قصور نصوص القانون الجنائي عن تحقيق الحماية دفع المشرع إلى اعتماد نصوص قانونية حديثة للقانون الجنائي، واعتماد نصوص خاصة تحقق الحماية لبعض الجرائم الأخرى.

اولا : الحماية الجنائية في نطاق مدونة القانون الجنائي

ان عدم كفاية نصوص القانون الجنائي، وأنه من الصعوبة بما كان تطبيق القواعد العامة التقليدية في القانون الجنائي على جرائم المس بنظم المعلوماتية دفع المشرع لتحديث قواعد هذا القانون. حيث تضمن القانون 03-07 كل من الجرائم التي تستهدف المس بنظم المعالجة كجريمة الدخول أو البقاء غير المشروع في النظام وجريمة عرقلة سير النظام أو احداث خلل فيه، ثم الجرائم التي تستهدف المعطيات والوثائق المعلوماتية.

أ: الجرائم التي تستهدف المس بنظم المعالجة الآلية للمعطيات

فالجريمة إما أن تكون "جريمة الدخول أو البقاء غير المشروع في النظام"، أو "عرقلة سيره وإحداث خلل فيه."

- **جريمة الدخول أو البقاء غير المشروع في النظام**

بالرجوع إلى مقتضيات الفصل 3-607 من القانون الجنائي المغربي نجده ينص على أركان جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات في صورتها البسيطة والمشددة، بحيث تمثل الصورة البسيطة لهذه الجريمة في مجرد الدخول أو البقاء غير المشروع حسب الفقرة الأولى والثانية من هذا الفصل، بينما تحقق الصورة المشددة حسبما بينت الفقرة الثالثة بتوافر الظرف المشدد لها، الذي يتمثل في أن الدخول أو البقاء غير المشروع يصاحبه إما محو أو تغيير في المعطيات الموجودة في النظام، وإما تعييب وظيفة تشغيل النظام.

ويتمثل الركن المادي في جريمة الدخول أو البقاء البسيطة في فعل الدخول إلى النظام المعالجة الآلية للمعطيات أو في جزء منه، وفي فعل البقاء في هذا النظام أو في جزء منه

هذا، ويلاحظ أن المشرعين الفرنسي والمغربي يعاقبان على الدخول المجرد إلى النظام المعلوماتي، ذلك أن مجرد الدخول غير المسموح به إلى النظام تقوم به الجريمة حتى ولو لم يترتب على دخوله ضرر، ولم يجن من ورائه أية فائدة

وتجدر الإشارة في الأخير إلى أن جريمة الدخول أو البقاء غير المشروع داخل النظام هي جريمة عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، ويستشف هذا من خلال تنصيص المشرع صراحة على ضرورة أن يكون الدخول عن طريق الاحتيال، ومن ثم

فإنه يلزم لكي يتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو البقاء، وأن يعلم الجاني أنه ليس له الحق في الدخول إلى النظام أو البقاء فيه، وذلك بغض النظر عن الباعث من وراء الدخول، هل هو تحقيق هدف مادي أو فقط بدافع الفضول أو التنزه أو إثبات القدرة على الانتصار على النظام، وبالإضافة إلى جريمة الدخول أو البقاء غير المشروع في النظام، هناك جريمة ثانية تدخل في إطار الجرائم التي تستهدف المس بنظم المعالجة الآلية للمعطيات، وهي جريمة عرقلة سير النظام أو إحداث خلل فيه.

- **جريمة عرقلة سير النظام أو إحداث خلل فيه**

ينص الفصل 5-607 من القانون الجنائي المغربي نجده يعاقب على كل فعل من شأنه عرقلة تشغيل نظام المعالجة الآلية للمعطيات أو أحدث فيه خللا مما أدى إلى اضطراب سيره، ويتمثل الركن المادي لهذه الجريمة في عرقلة سير النظام أو إحداث خلل فيه، ولا يشترط أن يقع فعل العرقلة أو فعل إحداث الخلل على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء في ذلك المادية، كجهاز الحاسوب، وشبكات الاتصال، وأجهزة الربط، وغيرها، والمعنوية كالبرامج...

وجريمة عرقلة سير نظام المعالجة الآلية للمعطيات أو إحداث خلل فيه هي جريمة قصدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه الإرادة إلى فعل عرقلة سير النظام أو إحداث خلل فيه.

وجدير بالذكر -ما دمنا نبحث في هذه الفقرة عن الجرائم التي تستهدف المس بنظم المعالجة الآلية للمعطيات- أن نستعرض نص الفصل 10-607 من القانون الجنائي المغربي، الذي ينص على معاقبة كل من صنع تجهيزات أو أدوات أو أعد برامج للمعلوميات أو أية معطيات أعدت أو اعتمدت خصيصا لأجل ارتكاب الجرائم المعاقب عليها في هذا الباب أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير

وبالإضافة الى الجرائم التي تستهدف المس بنظم المعالجة الآلية للمعطيات السالفة الذكر، توجد جرائم تستهدف المعطيات والوثائق المعلوماتية.

ب: الجرائم التي تستهدف المعطيات والوثائق المعلوماتية

بالنسبة للجرائم التي تستهدف المعطيات، وتزوير الوثائق المعلوماتية واستعمالها، فإنها تعتبر من الجرائم الحديثة التي نظمها المشرع في القانون الجنائي.

- **الجرائم التي تستهدف المعطيات**

يتمثل النشاط الاجرامي في الجرائم التي تستهدف الاعتداء على المعطيات عن طريق الاحتيال كما هو واضح من نص الفصل 6-607 في إدخال معطيات في نظام المعالجة الآلية للمعطيات، واتلاف أو حذف معطيات في نظام المعالجة الآلية للمعطيات، وتغيير المعطيات المدرجة في نظام المعالجة الآلية المعطيات، أو تغيير طريقة معالجتها أو طريقة إرسالها.

- ادخال المعطيات: يتحقق فعل الإدخال بإضافة معطيات جديدة إلى النظام الخاص بها الشيء المادي سواء أكان خاليا أم كان يوجد به معطيات من قبل، وهذه الجريمة تقع غالبا بمعرفة موظفي قسم المعلوميات الذين يقومون بوظائف المحاسبة والمعاملات المالية، لأنهم يكونون في أفضل وضع يؤهلهم لارتكاب هذا النمط من التلاعب غير المشروع.
- إتلاف أو حذف المعطيات: إزالة كل جزء من المعطيات المسجلة على دعامة، والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكر
- تغيير المعطيات أو تغيير طريقة معالجتها أو إرسالها: تغيير المعطيات الموجودة داخل النظام واستبدالها بأخرى بهدف الحصول على نتائج مغايرة عن تلك التي صمم النظام من أجلها.

➢ **جريمة تزوير الوثيقة المعلوماتية واستعمالها**

يعرف التزوير في مجال نظام المعطيات، بوصفه أحد أنماط الغش المعلوماتي تزايدا سريعا في الآونة الأخيرة، وذلك بالقدر الذي تحل فيه المحررات الإلكترونية محل المستندات العادية في جميع المجالات، حيث أصبحت الوثيقة المعلوماتية تحظى بأهمية كبيرة في الحياة العامة، حيث عمل المشرع على حمايتها بالفصل 7-607 الذي نص صراحة على معاقبة كل من زور أو زيف وثائق المعلوميات أيا كان شكلها، إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير، ناهيك عن معاقبة كل من استعمل وثائق المعلوميات المزورة أو المزيفة وهو يعلم أنها كذلك.

ولتحقق الجريمة لابد من توفر شرطين وجود مساس مادي بتغيير حقيقية الوثيقة المعلوماتية، ثم أن يتسبب هذا الأمر في ضرر للغير وهو ما نص عليه صراحة الفصل السابق الذكر.

وتأسيسا على ما سبق يتضح أن المشرع المغربي عالج جريمة تزوير الوثيقة المعلوماتية باعتبارها جريمة مستقلة عن جرائم التزوير العادية المتعلقة بالأوراق الرسمية والعمومية أو الأوراق العرفية أو المتعلقة بالتجارة والبنوك أو أنواع خاصة من الوثائق الإدارية والشهادات وغيرها[1].

[11] - عبد الرحمن فضل جمعة ادم : الجريمة المعلوماتية في نطاق حقوق المؤلف و الحقوق المجاورة، بحث نهاية التكوين بالمعهد العالي للقضاء سنة 2016/2015 ، ص7

الفقرة الخامسة: الحماية الجنائية خارج مدونة القانون الجنائي

إن التقدم العلمي بالمعنى الدقيق يبقى همجيا وفوضويا إذا لم يأطره ولم يواكبه تقدم فكري وقانوني، خاصة في شقه الزجري، وهذا ما تنبه له المشرع المغربي بمناسبة إصداره لأي مقتضيات قانونية تنظم مجالا يهم المسائل العلمية أو التكنولوجية الحديثة، وفي مقدمتها القوانين المتعلقة بالمعطيات، كالقانون رقم 53.05 المتعلق بالتبادل الالكتروني للمعطيات القانونية، والقانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي، فضمنها عدة مقتضيات زجرية، ويقتضي منا التطرق بداية لكل من الحماية الجنائية من خلال قانون المؤلف والحقوق المجاورة، على أن نتطرق لباقي القوانين الأخرى.

أ- الحماية الجنائية للمعطيات من خلال حق المؤلف

لقد صدر القانون رقم 34.05 ليغير ويتمم القانون رقم 2.00 المتعلق بحقوق المؤلف والحقوق المجاورة، وما يهمنا في هذا القانون هو النصوص المتعلقة بالمس بأنظمة المعالجة الآلية للمعطيات، خصوصا المادة 65 منه باعتبار شمولها للعديد من الجرائم التي ترتبط بموضوع هذا البحث.

وبالرجوع إلى المادة الثانية من القانون رقم 34.05 نجدها تنص على أنه يستفيد كل مؤلف من الحقوق المنصوص عليها في هذا القانون على مصنفه الأدبي والفني، وأن هذه الحماية تبدأ بمجرد إيداع المصنف، حتى ولو كان غير مثبت على دعامة مادية.

إن الأنظمة التقنية تم تصميمها خصيصا لحماية هذه المصنفات، لذلك فالمساس بهذه الأنظمة يشكل اعتداء خطيرا معاقبا عليه، ويمكن إجمال هذه الاعتداءات في صورتين، الصورة الأولى جريمة قض مفاتيح التشفير، والثانية جريمة المس بالبيانات المشفرة.

فيما يخص جريمة فض مفاتيح التشفير، فإنه لابد من وجود مصنف محمي له صاحب الحق حتى يكتمل الركن المادي لهذه الجريمة، والمصنف المحمي هنا هو برنامج الحاسوب، وقواعد البيانات، حيث أصبحت المصنفات المعالجة آليا تمتع بحماية قانون المؤلف والحقوق المجاورة

وهكذا فإنه لا يستفيد من هذه الحماية إلا المصنف الذي يعكس شخصية من ينسب إليه حيث يعد ابتكارا له يخوله ذلك الحق، والابتكار يعني أن المصنف يتميز بطابع أصيل، أي أن يكون المؤلف قد أضاف من عبقريته إلى فكرة سابقة ما يجعل لها طابعا جديدا يسمح بتمييز المصنف عما كان عليه من قبل سواء أتعلق ذلك بجوهر الفكرة أم تعلق بطريقة عرضها، أم بالتعبير عنها أم بترتيبها.....

ب-الحماية الجنائية للمعطيات على ضوء بعض القوانين الحمائية الأخرى

لقد سعى المشرع المغربي إلى تهيئة بيئة قانونية تتناسب والتطور الهائل المذهل في مجال التبادل الالكتروني للمعطيات الذي أصبح يتم من خلال الانترنيت، ومن ثم الانتقال من مرحلة التعامل الورقي إلى مرحلة التعامل الالكتروني، ويأتي في هذا السياق صدور القانون رقم 53.05.

وإذا كان القانون رقم 53.05 أثُر بشكل أساسي على فصول قانون الالتزامات والعقود المغربي بفعل تعديل بعض نصوصه أو إضافة أخرى جديدة متصلة بالبيئة الالكترونية، إلا انه يتضمن كذلك مجموعة من النصوص الزجرية، والتي تساهم في الحماية الجنائية للتبادل الالكتروني للمعطيات، نذكر منها المادة 29 التي تعاقب كل من يقدم خدمات للمصادقة الالكترونية المؤمنة خلافا للمادة 20 منه أو دون أن يكون متعمدا أو من يواصل نشاطه رغم سحب اعتماده، أما المادة 31 فتعاقب على الادلاء العمدي بتصاريح كاذبة أو تسليم وثائق مزورة إلى مقدم خدمات المصادقة الالكترونية.

ومن أجل ضمان سلامة تبادل المعطيات القانونية بطريقة الكترونية وضمان سريتها وصحتها، فرض المشرع حماية خاصة لوسائل التشفير من خلال المادة 32 التي تجرم استيراد أو استغلال أو استعمال إحدى الوسائل أو خدمة من خدمات التشفير دون الادلاء بالتصريح أو الحصول على الترخيص، كما أنه يمكن للمحكمة الحكم بمصادرة وسائل التشفير المعنية

كما جرم المشرع المغربي كل استعمال لوسيلة تشفير لتمهيد أو ارتكاب جناية أو جنحة، أو لتسهيل تمهيدها أو ارتكابها لكن ذلك لا يطبق على مرتكب الجريمة أو المشارك في ارتكابها الذي يسلم إلى السلطات القضائية أو الإدارية، بطلب منها، النص الواضح للرسائل المشفرة وكل ما يلزم لقراءة النص المشفر

ولتحقيق الحماية الجنائية للتوقيع الالكتروني عاقبت المادة 35 كل استعمال غير قانوني للعناصر الشخصية لإنشاء التوقيع المتعلقة بتوقيع الغير، كما حمى المشرع المغربي، من خلال المادة 37، حجية الشهادة الالكترونية عير تجريم الاستمرار في استعمالها بعد مدة صلاحيتها أو بعد إلغائها

وقد سار المشرع المغربي مع التوجه التشريعي فأصدر كذلك القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي، وما يهمنا في هذا القانون هو الباب السابع الخاص بالعقوبات ومنه المواد 53-63 المتعلقة حالة رفض المسؤول معالجة حقوق الولوج أو حالة نقل معطيات ذات طابع شخصي نحو دولة أجنبية، كما تطريق لحالات الاستعمال التعسفي أو التدليسي للمعطيات أو ايصالها لأغيار غير مؤهلين من طرف المسؤول عن المعالجة.

وارتباطا كذلك بمسألة مكافحة الجرائم المعلوماتية، فقد وضع المشرع مقتضيات زجرية تنظم الجرائم الجمركية التي تنجز بطرق الكترونية ضمن القسم الأول من الباب الثالث، حيث ورد في الفقرة السابعة من الفصل 281 من مدونة الجمارك

وعليه يكون هذا الفصل قد حسم في مسألة اعتبار المعلومات المخزنة بالحاسب الآلي نوعا من الوثائق الإدارية[1].

الفرع الثاني: الجريمة المعلوماتية او الإلكترونية في القوانين المصرية

بالنظر الى مجهودات البرلمان المصري تجاه محاربة ومكافحة جرائم تقنية المعلومات، أخيرا صدر قانون مكافحة جرائم تقنية المعلومات، وتضمن للمرة الاولى تجريم الممارسات الالكترونية غير المشروعة، والتي لا يوجد ما يجرمها في القانون المصري، ومنها التزوير الالكتروني وإنشاء مواقع للتشجيع على الارهاب أو نقل المعلومات، وتتراوح العقوبات في هذا القانون حسب جسامة الجريمة، في حالة جرائم تقنية المعلومات التي يترتب عليها تهديد الامن القومي والسلم الاجتماعي، إضافة إلى عقوبات الاختراق الالكتروني والتزوير وغيرها من الجرائم، كما ينص هذ القانون على عقوبات لبعض جرائم تقنية المعلومات تتضمن حجب مواقع أو إلغاء تراخيصها بأحكام قضائية.

الفقرة الاولى: الاحكام العامة الواردة في قانون مكافحة جرائم تقنية المعلومات المصري

صدر القانون 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، متضمنا في مادته الاولى من الباب الاول التعريفات والمصطلحات المستخدمة والمرتبطة بقواعد واحكام هذا القانون الجديد. حيث جرى نص المادة الاولى من الباب الاول بشأن الاحكام العامة لتطبيق القانون تحت عنوان "تعريفات" على ان:

في تطبيق أحكام هذا القانون، يقصد بالألفاظ والعبارات الاتية المعنى المبين قرين كل منها:

- الجهاز : الجهاز القومي لتنظيم الاتصالات
- الوزير المختص : الوزير المعنى بشئون الاتصالات وتكنولوجيا المعلومات.
- البيانات والمعلومات الالكترونية : كل ما يمكن إنشاؤه أو تخزينه، أو معالجته، أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات، كالأرقام والاكواد والشفرات والحروف والرموز والاشارات والصور والاصوات وما في حكمها.

[1] - عبد الكريم غالي: قانون المعلومات الحماية القانونية للإنسان من مخاطر المعلومات ، أطروحة لنيل دكتوراه الدولة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية و الاقتصادية و الاجتماعية بالرباط، السنة الجامعية 1994/1995 ، ص6

- بيانات شخصية : أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى.
- بيانات حكومية : بيانات متعلقة بالدولة أو أحد سلطاتها، وأجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة والاجهزة الرقابية، وغيرها من الاشخاص الاعتبارية العامة وما فى حكمها، والمتاحة علي الشبكة المعلوماتية أو علي أي نظام معلوماتي أو على حاسب أو ما في حكمها.
- المعالجة الالكترونية : أي عملية إلكترونية أو تقنية تتم كلياً أو جزئيا، لكتابة، أو تجميع، أو تسجيل، أو حفظ ، أو تخزين، أو دمج، أو عرض، أو إرسال، أو استقبال، أو تداول، أو نشر، أو محو، أو تغيير، أو تعديل ، أو استرجاع ، أو استبدال للبيانات والمعلومات الالكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الاجهزة الاخرى الالكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخرى.
- تقنية المعلومات : أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً.
- مقدم الخدمة : أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات.
- المستخدم : كل شخص طبيعي أو اعتباري، يستعمل خدمات تقنية المعلومات أو يستفيد منها بأي صورة كانت.
- البرنامج المعلوماتي : مجموعة الاوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الاشكال،

ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة سواء كانت هذه الاوامر والتعليمات في شكلها الاصلي أو في أي شكل آخر تظهر فيه من خلال الحاسب الآلي، أو نظام معلوماتي.

- النظام المعلوماتي : مجموعة برامج وأدوات معدة لغرض إدارة ومعالج البيانات والمعلومات، أو تقديم خدمة معلوماتية.

- شبكة معلوماتية : مجموعة من الاجهزة أو نظم المعلومات مرتبطة معاً ، ويمكنها تبادل المعلومات والاتصالات فيما بينها ، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها.
- الموقع: نطاق أو مكان افتراضي له عنوان محدد على شبكة معلوماتية.
- مدير الموقع : هو كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ علي موقع أو أكثر على الشبكة المعلوماتية، بما فيها حقوق الوصول لمختلف المستخدمين علي ذلك الموقع أو تصميمه، أو توليد وتنظيم صفحاته أو محتواه أو المسئول عنه.
- الحساب الخاص: مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له الحق دون غيره الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي

.

- البريد الالكتروني : وسيلة لتبادل رسائل إلكترونية على عنوان محدد ، بين أكثر من شخص طبيعي أو اعتباري ، عبر شبكة معلوماتية ، أو غيرها من وسائل الربط الالكترونية، من خلال أجهزة الحاسب الآلي وما في حكمها.
- الاعتراض : مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل ، أو تغيير المحتوى ، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق.
- الاختراق : الدخول غير المرخص به، أو المخال لأحكام الترخيص ، أو الدخول بأي طريقة غير مشروعة ، إلي نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية، وما في حكمها.
- المحتوي : أي بيانات تؤدي بذاتها، أو مجتمعه مع بيانات أو معلومات أخرى إلي تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معني أو الاشارة إلي بيانات أخري.
- الدليل الرقمي : هو أية معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها ، والممكن تجميعه وتحليله باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.
- الخبرة : كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل في مجالات تقنية المعلومات.

- حركة الاتصال (بيانات المرور): بيانات ينتجها نظام معلوماتي تبين مصدر الاتصال، وجهته والوجهة المرسل منها وإليها، والطريق الذي سلكه، وساعته وتاريخه وحجمه ومدته، ونوع الخدمة.
- الحاسب : كل جهاز أو معدة تقنية تكون قادرة على التخزين، أو اداء عمليات منطقية، أو حسابية، وتستخدم لتسجيل بيانات أو معلومات، أو تخزينها، أو تحويلها، أو تخليقها، أو استرجاعها، أو ترتيبها، أو معالجتها، أو تطويرها، أو تبادلها، أو تحليلها، أو للاتصالات.
- دعامة إلكترونية: أي وسيط مادي لحفظ وتداول البيانات والمعلومات الالكترونية ومنها الأقراص المدمجة أو الاقراص الضوئية أو الذاكرة الالكترونية أو ما في حكمها.
- الامن القومي : كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أرضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الامن القومي، ووزارة الدفاع والانتاج الحربي، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الادارية، والاجهزة التابعة لتلك الجهات.
- جهات الامن القومي : رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية.

وحيث ان المادة الاولى من قانون مكافحة تقنية المعلومات، لها من الاهمية، مما يتعين التعرض لما ورد بها من أحكاما عامة، يجب مراعاتها بشأن تطبيق احكام هذا القانون.

الفقرة الاولى: موقف المشرع المصري من تعريف جرائم تقنية المعلومات

لا شك ان الفقه القانوني يفضل ان يتفادى المشرع غالبا التسرع إلى وضع تعريفات للظواهر القانونية الجديدة، لأنها تميز بالتغير والتقلب وعدم الثبات، حتى لا يكون التعريف بمثابة مجازفة ليست مأمونة العواقب، ومع ذلك نالت جرائم تقنية المعلومات اهتماما كبيرا من جانب الفقه الجنائي الذي خصص لها تعريفات متعددة وانطلق في اطارها من زوايا متعددة. فقد ترك المشرع المصري تعريف جرائم تقنية المعلومات للاجتهادات الفقهية، وذلك وفقا لما ينجم عنه التطور التكنولوجي المعاصر، وتأثيره على الظاهرة الاجرامية محل التعريف، ومكتفيا بتحديد وتعريف كافة الافعال المقترنة بتلك الجرائم.

وحيث ان المشرع المصري في القانون الجديد بشأن مكافحة جرائم تقنية المعلومات، عرف في مادته الاولى، الحاسب على انه : كل جهاز أو معدة تقنية تكون قادرة على التخزين، أو اداء

عمليات منطقية، أو حسابية، وتستخدم لتسجيل بيانات أو معلومات، أو تخزينها، أو تحويلها، أو تخليقها، أو استرجاعها، أو ترتيبها، أو معالجتها، أو تطويرها، أو تبادلها، أو تحليلها، أو للاتصالات.

وعرف الدعامة الالكترونية، بانها: أى وسيط مادى لحفظ وتداول البيانات والمعلومات الالكترونية ومنها الاقراص المدمجة أو الاقراص الضوئية أو الذاكرة الالكترونية أو ما في حكمها.

وقد تبنى المشرع المصري في القانون الجديد، الرأى الذى يتجه الى عدم وضع تعريف محددا لجرائم تقنية المعلومات، تاركا تعريف تلك النوعية من الجرائم الى الفقه الجنائي، فى ظل ما يتمخض عليه ارض الواقع من تطور تكنولوجى، يكون له بالغ الاثر على تلك الجرائم، وحتى لا يكون التعريف مرتبطا بحقبة زمنية معينة، قد تتغاير التقنيات التكنولوجية المستخدمة فى جرائم تقنية المعلومات، نظرا لتسارع وتيرة تطورها.

واتجاه المشرع المصري، فى شأن عدم وضع تعريف محدد لجرائم تقنية المعلومات، هو اتجاه محمود، للأسباب السابقة، ويضاف الى ذلك، ان الفقه الجنائي جدير بوضع هذا التعريف، وتغييره حسبما يستجد من تطورات وتقنيات تكنولوجية، من شانهما تغيير المفهوم والتعريف المقترح لجرائم تقنية المعلومات.

وبالرجوع الى مؤتمر الامم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، يتضح انه تبنى تعريف منضبط لجريمة تقنية المعلومات بأنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسبي أو شبكة حاسبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية."

الجريمة المعلوماتية: كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون.

الفقرة الثانية: الجرائم والعقوبات في القانون المصري

مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر، ومراعاة أحكام قانون الطفل رقم 12 لسنة 1996 والمعدل بالقانون 126 لسنة 2008، يعاقب العقوبات المبينة قرين كل جريمة،

اولا: الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

- ✓ **جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها :** يعاقب بالحبس مدة لا تقل عن 3 شهور وبغرامة لا تقل عن 10 ألف جنيه ولا تجاوز 50 ألف جنيه أو بأحدي هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي، أو إحدى وسائل تقنية المعلومات، بخدمة من خدمات اتصالات أو خدمات قنوات البث المسموع والمرئي.
- ✓ **جريمة تجاوز حدود الحق في الدخول :** يعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 30 ألف جنيه ولا تجاوز 50 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول.
- ✓ **جريمة الدخول غير المشروع :** يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن 50 ألفا ولا تجاوز 100 ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل عمدا أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.

فإذا أنتج عن ذلك إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 200 ألف أو بإحدى هاتين العقوبتين.

- ✓ **جريمة الاعتراض غير المشروع :** يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 250 ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الألى وما في حكمها.
- ✓ **جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية :** يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن100 ألف جنيه ولا تجاوز 500 ألف جنيه، أو بإحدى هاتين العقوبتين كل من أتلف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة.

- ✓ **جريمة الاعتداء على البريد الإليكتروني أو المواقع أو الحسابات الخاصة :** يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 100 ألف جنيه أو بإحدى العقوبتين كل من أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بأحد الناس.

فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى هاتين العقوبتين.

- ✓ **جريمة الاعتداء على تصميم موقع :** يعاقب بالحبس مدة لا تقل عن 3 أشهر، وبغرامة لا تقل عن 20 ألف جنيه ولا تجاوز 100 ألف جنيه أو بإحدى العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوه أو اخفى، أو غير تصاميم موقعاً خاصاً بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق.

- ✓ **جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة :** يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا أو بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها.

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية تكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه.

وفى جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغائها كليا أو جزئيا بأي وسيلة كانت، تكون العقوبة السجن والغرامة التى لا تقل عن مليون جنيه ولا تجاوز 5 ملايين جنيه.

- ✓ **جريمة الاعتداء على سلامة الشبكة المعلوماتية :** يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها، أو الحد من كفاءة عملها، أو التشويش عليها، أو إعاقتها، أو اعتراض عملها، أو أجرى بدون وجه حق معالجة الكترونية للبيانات الخاصة بها.

ويعاقب كل من تسبب بخطاه في ذلك، بالحبس مدة لا تقل عن ثلاث شهور، وبغرامة لا تقل عن خمسون ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى العقوبتين. فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة، أو تدار بمعرفتها أو تمتلكها، تكون العقوبة السجن المشدد وبغرامة لا تقل عن خمسمائة ألف جنيه ول اتجاوز مليون جنيه.

- ✓ **البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات:** يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 300 ألف جنيه ولا تجاوز 500 ألف جنيه أو بإحدى العقوبتين كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول أي جهاز أو معدات أو برامج أو أكواد مرور أو شفرات أو أي بيانات مماثل، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أية جريمة من المنصوص عليها في هذا القانون أو إخفاء أثرها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء.

ثانيا : الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات

- ✓ **جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني :** يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الالكترونية

فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن 6 أشهر وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز 200 ألف، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير.

- ✓ **الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني :** يعاقب بالحبس مدة لا تقل عن 3 أشهر وغرامة لا تقل عن 10 آلاف جنيه ولا تجاوز 30 ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريدا إلكترونيا أو موقعا أو حاسبا خاصا ونسبه زورا لشخص طبيعي أو اعتباري.

فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسئ إلى من نسب إليه، تكون العقوبة الحبس الذى لا تقل مدته عن سنة وغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة فتكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تزيد على 300 ألف جنيه.

- ✓ **الجرائم المتعلقة بالاعتداء على حرمه الحياة الخاصة والمحتوى المعلوماتي غير المشروع :** يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الاسرية في المجتمع المصري، أو انتهك حرمة الحياه الخاصة أو ارسل بكثافة العديد من الرسائل الاليكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع الكتروني لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو اخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة ام غير صحيحة.

- ✓ **يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز** خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز 300 ألف جنيه أو بإحدى العقوبتين كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها لا بمحتوى مناف للآداب العامة أو لإظهارها بطريقة من شانها المساس باعتباره أو شرفه.

ثالثا : الجرائم المرتكبة من مدير الموقع

- ✓ في غير الأحوال المنصوص عليها فى هذا القانون، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 ألف جنيه ولا تزيد عن 300 ألف جنيه أو بإحدى هاتين العقوبتين، كل من أنشا أو أدار أو استخدم موقعا أو حسابا خاصا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً.
- ✓ يعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 20 ألف ولا تجاوز 200 ألف أو إحداي هاتين العقوبتين، كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها فى هذا القانون والتي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة.
- ✓ يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن 20 ألف ولا تجاوز 200 ألف جنية، أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإليكتروني أو النظام المعلوماتي عرض أي منهم لإحدى الجرائم المنصوص عليها في هذا القانون.
- ✓ ويعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 10 الاف جنية ولا تجاوز 100 ألف جنية أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإليكتروني أو النظام المعلوماتي، تسبب بإهماله في تعرض أي منهم لإحدى الجرائم المنصوص عليها في هذا القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطات التأمينية الواردة في اللائحة التنفيذية.

رابعا : المسؤولية الجنائية لمقدمي الخدمة

- ✓ يعاقب بالحبس مدة لا تقل عن سنة والغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون أو إحدى هاتين العقوبتين كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من

المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه في الفقرة الأولى من المادة 7 من هذا القانون.

فإذا ترتب على الامتناع عن تنفذ القرار الصادر من المحكمة وفاة شخص أو أكثر أو الأضرار بالأمن القومي وتكون العقوبة السجن المشدد وغرامه لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضى المحكمة فضلا عن ذلك بإلغاء ترخيص مزاولة المهنة.

- ✓ يعاقب بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام الواردة بالبند (2) من الفقرة أولا من المادة (2) من هذا القانون، وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمى الخدمة.
- ✓ يعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 20 ألف جنيه ولا تجاوز 100 ألف جنية أو بإحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من بيانات أو معلومات المشار إليها فى المادة (6) من هذا القانون.
- ✓ يعاقب بغرامة لا تقل عن 5 ملايين جنية ولا تجاوز 10 ملايين، كل مقدم خدمة أخل بأي من التزاماته المنصوص عليها فى البند (1) من الفقرة أولاً من المادة (2) والفقرة الثانية من البند رابعاً من هذا القانون. وتضاعف عقوبة الغرامة فى حالة العود، وللمحكمة القضاء بإلغاء الترخيص.
- ✓ يعاقب مقدمو الخدمة بالحبس مدة لا تقل عن 3 أشهر وبالغرامة التي لا تقل عن 200 ألف جنية ولا تجاوز مليون جنية كل من خالف أحكام الفقرة ثالثاً من المادة (2) من هذا القانون.

خامسا : الظروف المشددة في الجريمة

- ✓ إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الاخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الاضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل احكام الدستور أو القوانين أو اللوائح أو الاضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد.

- ✓ يعاقب بالحبس مدة لا تقل عن 3 أشهر وبغرامة لا تقل عن 30 ألف جنية ولا تزيد عن 100 ألف جنية أو بإحدى هاتين العقوبتين، كل مسئول عن الإدارة الفعلية لأى شخص اعتباري، إذا تعرض الموقع أو الحساب الخاص أو البريد الإليكتروني أو النظام المعلوماتي المخصص للكيان الذى يديره، لأى جريمة من الجرائم المنصوص عليها في هذا القانون، ولم يبلغ بذلك الجهات المختصة وقت علمه بالجريمة.
- ✓ في الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون، باسم ولحساب الشخص الاعتباري، يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي. وللمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتبار للنشاط مدة لا تزيد على سنة، ولها في حاله العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري.
- ✓ في تطبيق أحكام هذا القانون، لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتباري استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التي تقوم بها الجريمة.

سادسا: العقوبات التبعية

- ✓ مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون، أن تقضى بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها.
- ✓ للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتا من وظيفته، إلا في الحالات المشار اليها في المادة (35) من هذا القانون فيكون العزل وجوبيا.

سابعا: الشروع والاعفاء من العقوبة

- ✓ كل من شرع في ارتكاب الجرائم المنصوص عليها بالقانون، يعاقب بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة.

- ✓ يعفى من العقوبات، المقررة للجرائم المنصوص عليها في هذا القانون، كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها.

ويجوز للمحكمة الاعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها، إذا مكن الجاني أو الشريك - في أثناء التحقيق - السلطات المختصة من القبض على مرتكبي الجريمة الأخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثله لهذا النوع والخطورة. ولا يخل حكم هذه المادة، بوجوب الحكم برد المال المتحصل من الجرائم المنصوص عليها بالقانون.

- ✓ **التصالح :** يجوز للمتهم في أية حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتاء، إثبات الصلح مع المجنى عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك في الجنح المنصوص عليها في المواد 15، 16،17، 18، 19، 20، 24، 27، 29، 31، 32، من هذا القانون. ولا ينتج اقرار المجنى عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد 15، 18، 19، 24 من هذا القانون.

كما لا يقبل التصالح إلا من خلال الجهاز بخصوص الجنح المنصوص عليها بالمادتين30، 36 من هذا القانون. ولا يسقط حق المتهم في التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثي الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر، وذلك قبل صدور حكم نهائي في الموضوع. وفى جميع الأحوال، يجب على المتهم الذى يرغب في التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغا يعادل ضعف الحد الأقصى للغرامة المقرر للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة بحسب الأحوال.

ويترتب على الصلح انقضاء الدعوى الجنائية، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية[1] .

المطلب الثاني: الجرائم الماسة بالإعلام الرقمي

[1] - قانون مكافحة جرائم تقنيات المعلومات أغسطس/ اب سنة 2018

كان من بين أهم نتائج الربيع العربي السعي إلى تطوير الإعلام الالكتروني وإعداد قوانين تنظمه وتحمي العاملين فيه، شأنهم شأن العاملين في الإعلام التقليدي. كما تم الاهتمام بالحق في الحصول على المعلومة و دسترتها ضمن مواد الدساتير العربية خاصة دساتير دول الحراك العربي

الفرع الأول: وضعية الإعلام الالكتروني وحق الحصول على المعلومات في مصر

الفقرة الأولى : الإعلام الرقمي في مصر

كان للإعلام الرقمي وخاصة الإعلام الاجتماعي أو Sociel Media وعلى رأسه الفيسبوك الدور الرئيسي في هذه التحولات الأخيرة ومازال يلعب دور الرقيب على المكتسبات الحاصلة في الساحة المصرية بداية بالإصلاحات السياسية وصولا إلى التشريعات والقوانين التي تم إرساؤها .

لكن هل كان للإعلام البديل أو الالكتروني مكانة في هذه الحملة الإصلاحية؟

لقد نص الدستور المصري الجديد بشكل مؤكد على ضرورة احترام حرية الصحافة والطباعة والنشر والإعلام الالكتروني ووسائط الإعلام الرقمي بشكل واضح في المادة 70 منه، وقد سبقت الإشارة إلى ذلك في الفقرات السابقة. لكن هل تم تفعيلها؟

في إطار تدعيم الإعلام الالكتروني واعترافا بدوره في الثورات العربية تم إشهار نقابة الصحفيين الالكترونيين المصرية بحسب قانون الحريات النقابية سنة 2011، وتم تدشين النقابة المهنية عقب إقرار لجنة الخمسين لتعديل الدستور، واقتراحه النقابة إضافة الصحافة الالكترونية إلى المواد الخاصة بالصحافة والإعلام في الدستور وهو ما منح النقابة الحق في تأسيس نقابة مهنية وذلك سنة 2013، كما قامت النقابة بإعداد ميثاق شرف مهني للصحفيين الالكترونيين يعتمد على العديد من المبادئ الأساسية مثل:

- احترام الميثاق العالمي لحقوق الإنسان والأعراف والقيم العربية؛
- الاحترام والالتزام بحق التعبير وحق الاطلاع والحصول على المعلومة؛
- احترام الخصوصيات وعدم المساس بالأمور الشخصية؛
- احترام حقوق الملكية الفكرية والفصل بين التحرير والإعلان .

أما بخصوص قانون ينظم الإعلام الالكتروني فهناك تخوف من طرف العاملين في هذا المجال من وضع قانون يقيد الحريات، وهناك من يستبشر خيرا أملا في الحصول على استحقاقات مهنية ومواد قانونية تحميهم من مخاطر وتحديات العمل في ظل ثقافة مجتمعية وحكومية مازالت لم تعترف بشكل واضح بالصحفي الإلكتروني وتضعف حقهم في الحصول على المعلومة ونشرها.

وللعلم يعمل الصحفي الالكتروني المصري حاليا بدون غطاء قانوني سوى الحماية التي تفرضها له المادة 70 من الدستور الجديد المصري ومن النقابة الوطنية للصحافة المصرية ومن بعض الوزارات، وهذا بعد أن يقوم الصحفي الالكتروني بتقديم طلب لهم. أما بخصوص قانون يحمي حق الحصول على معلومة فهناك مسودة قانون تنتظر الموافقة عليها من قبل البرلمان.

وأخطر ما قد يواجهه الصحفي الالكتروني المصري هي مواد قانون الإرهاب الذي تم المصادقة عليه في 16 من شهر شتنبر2015، حيث تنص المادة 29 من القانون على عقوبة السجن المشدد لمدة لا تقل عن خمس سنوات لكل من أنشأ أو استخدم موقعا الكترونيا «بغرض الترويج للأفكار والمعتقدات الداعية إلى ارتكاب أعمال إرهابية». وتسمح هذه المادة الفضفاضة للدولة العسكرية أن تستعملها بشتى الطرق للضغط على المدونين والصحفيين الالكترونيين، والقاء القبض عليهم وتخويفهم. طبعا هذا يخالف نص الدستور المصري وكل المعاهدات الدولية التي صادقة عليها الجمهورية العربية المصرية .

الفرع الثاني: المغرب: تأهيل الصحافة الالكترونية والحق في الحصول على المعلومات

- **العقوبات ضد الصحافة الإلكترونية**

إذا أضيفت العقوبات والغرامات التي تتعقب زلات الصحافة الإليكترونية إلى هذه العراقيل التي يعيشها القطاع عرف المتتبع للمشهد الإعلامي في المغرب؛ أي مستقبل ينتظر الصحافة الإليكترونية بالمغرب، وهي عقوبات كثيرة نكتفي بالإشارة إلى بعضها:

حسب المادة 24 يعاقب بغرامة مالية تتراوح بين 2.000 و10.000 درهم مالك المطبوع الدوري أو المستأجر المسير له، وعند عدم وجودهما مدير النشر، وعند عدمه صاحب المطبعة، وعند عدمه موزع المطبوع الدوري، الذي لم يكن موضوع تصريح طبقا لمقتضيات المادتين 21 و22 أعلاه، أو استند في إصداره على تصريح أصبح عديم الأثر طبقا لمقتضيات المادة 23 أعلاه. لا يمكن استمرار نشر المطبوع الدوري إلا بعد القيام بالإجراءات المنصوص عليها في المادة 21 أعلاه. في حالة الامتناع عن القيام بالإجراءات المذكورة، يعاقب الأشخاص الواردين في الفقرة الأولى أعلاه بالتضامن بغرامة قدرها 20.000 درهم يؤذونها عند كل نشر جديد غير قانوني، وتحتسب عن كل عدد ينشر ابتداء من يوم النطق بالحكم إذا صدر حضوريا أو ابتداء من اليوم الثالث الموالي لتبليغ الحكم إذا صدر غيابيا ولو كان هناك طعن. تتعرض الصحيفة الإلكترونية في حالة عدم التصريح بإحداثها لنفس العقوبة المشار إليها في الفقرة الأولى أعلاه وتتعرض كذلك للحجب إلى حين القيام بالإجراءات المنصوص عليها في المادة 21 أعلاه.«

وحسب ما جاء في المادة 81 «يعاقب بغرامة من 100.000 إلى 300.000 درهم على المس بشخص وكرامة رؤساء الدول ورؤساء الحكومات ووزراء الشؤون الخارجية للدول الأجنبية، بواسطة إحدى الوسائل المنصوص عليها في المادة 77 أعلاه». وحسب المادة 82 من نفس القانون «يعاقب بغرامة 50000 درهم إلى 200.000 درهم على المس بشخص وكرامة الممثلين الدبلوماسيين أو القنصليين الأجانب المعتمدين أو المندوبين لدى جلالة الملك، بواسطة إحدى الوسائل المنصوص عليها في المادة 77 أعلاه. بغرامة من 10.000 إلى 100.000 درهم عن القذف الموجه للأفراد بإحدى الوسائل المبينة في المادة 72 أعلاه». وفي المادة 84 «يعاقب بغرامة من 100.000 إلى 200.000 درهم، عن كل قذف يرتكب بإحدى الوسائل المبينة في المادة 72 أعلاه، في حق المجالس أو الهيئات القضائية أو المحاكم أو الجيوش البرية أو البحرية أو الجوية أو الهيئات المؤسسة أو المنظمة أو الإدارات العمومية بالمغرب، أو في حق وزير أو عدة وزراء، من أجل مهامهم أو صفاتهم أو في حق موظف أو أحد رجال أو أعوان السلطة العمومية أو كل شخص مكلف بمصلحة أو مهمة عمومية مؤقتة كانت أم مستمرة أو مساعد قضائي أو شاهد من جراء تأدية شهادته. يعاقب بغرامة من5.000 إلى 20.000 درهم على السب والإهانة الموجه بنفس الوسائل إلى الهيئات والأشخاص المنصوص عليهم في الفقرة الأولى أعلاه.

هذه مجرد عينة من الغرامات والعقوبات -وغيرها كثير- التي تنتظر الصحف الإليكترونية، والمتهمون فيها حسب المادة 95 «يعاقب بصفته فاعلا أصليا صاحب المادة الصحفية أو واضع الرسم أو الصورة أو الرمز أو بواسطة وسيلة إليكترونية أو طرق التعبير الأخرى أو المستورد أو الموزع أو البائع أو مقدمو الخدمات أو المضيف وذلك بحسب تراتبية المسؤولية المشار إليها في الفقرة الأولى من هذه المادة». وبتركيزه على العقوبة بالغرامات كان هذا القانون أقرب إلى قانون جنائي منه إلى قنان للصحافة والنشر لأن بعض البنون تتيح أمكانية أن يتابع الصحفي بالقانون الجنائي بل حتى بقانون الإرهاب وإن تم التخلي عن العقوبات الحبسية... ويضاف إلى هذه العقوبات المالية عدد من المواد في هذا القانون التي تعطي الحق للسلطة القضائية في إمكانية الحجب المؤقت أو الدائم لجريدة الإليكترونية ولا يتسع المجال هنا لسردها لأننا اقتصرنا على نقطتي التأسيس والغرامات ذلك أن هاتان النقطتان تفتحان باب الاجتهاد الذي قد لا تنجو منه أية جريدة إلكترونية، فكتابة أي مقال حول تقصير مسؤول في أداء مسؤوليته أو شططه في استعمال السلطة يمكن أن يؤول كتشهير أو قذف، وقد يتسبب في عقوبات مالية على جريدة إليكترونية لا يجني منها صاحبها شيئا... ومن تمت يمكن أن يرى البعض في هذا القانون تعارضا مع المعايير

الدولية لأنه يشترط شروطا ستجعل الآلاف من الجرائد الإليكترونية النشيطة اليوم في خبر كان. كما أن الحصول على البطاقة المهنية ينبغي أن يكون معكوسا، فعلى المرء أن يكون صحفيا وصاحب مقاولة إليكترونية نشيطة في الصحافة ليحصل على البطاقة المهنية، وليس أن يحصل على البطاقة أولا ليؤسس مقاولته ويشتغل في الصحافة... كما أن اشتراط الإجازة كحد تعليمي أدنى سيقضي على الأحلام الصحفية لعدد من نشطاء الميدان الذين لم تسعفهم الظروف على مواصلة دراساتهم العليا وربما هم الأكثرية ممن يمارسون في القطاع في ظل غياب معطيات دقيقة . ...

- **قانون 31,13 المتعلق بالحق في الحصول على المعلومات**

يعتبر حق الحصول على المعلومات حقا من الحقوق والحريات الأساسية التي نص عليها الدستور الصادر بتنفيذه الظهير الشريف رقم 1.11.91 بتاريخ 29 يوليوز 2011، ولاسيما الفصل 27 منه.

إن تكريس هذا الحق يأتي ليؤكد الالتزام الدائم للمملكة المغربية بحقوق الإنسان كما هي متعارف عليها عالميا، وبمقتضيات المادة 19 من الإعلان العالمي لحقوق الإنسان، والمادة 19 من العهد الدولي للحقوق المدنية والسياسية، وكذا المادة 10 من اتفاقية الأمم المتحدة لمكافحة الفساد التي ألزمت الإدارات العمومية بضرورة تمكين المواطنين من الحصول على المعلومات واتخاذ التدابير الكفيلة لممارستهم لهذا الحق، تعزيزا للشفافية وترسيخا لثقافة الحاكمة الجيدة.

واعتبارا للأهمية القصوى التي يكتسبها حق الحصول على المعلومات في تعميق الديمقراطية قيما ومبادئ وممارسة، يأتي قانون الحق في الحصول على المعلومات ليشكل ترجمة فعلية وملموسة لتنزيل مقتضيات الدستور ومتطلباته القانونية والمؤسساتية، وتعبيرا واضحا عن إرادة سياسية أكيدة تستجيب للحاجيات التي عبر عنها التطور الكمي والنوعي للإدارة والمجتمع.

ومن جهة أخرى سيسهم هذا القانون بحظ أوفر في ترسيخ دولة الحق والقانون، وفي تقوية الصرح التشريعي وتعزيز اللبنات القانونية الأخرى التي وضعها المغرب على هذا المسار ب :

- إصدار قانون إلزام الإدارات العمومية والجماعات المحلية والمؤسسات العمومية بتعليل قراراتها الإدارية،
- إصدار قانون حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي،
- إحداث مؤسسة الأرشيف ومؤسسة الوسيط والمجلس الوطني لحقوق الإنسان والهيئة المركزية للوقاية من الرشوة.

كما يهدف هذا القانون إلى :

- تدعيم وتقوية البحث العلمي والحقل المعرفي؛
- إشاعة ودعم قواعد الانفتاح والشفافية؛
- تعزيز الثقة في علاقة الإدارة بالمتعاملين معها؛
- ترسيخ الديمقراطية التشاركية؛
- إرساء إجراءات كفيلة بتخليق الممارسة الإدارية؛
- ضمان المصداقية والنزاهة في تدبير الشأن العام؛
- فهم أفضل للإجراءات والمساطر الإدارية من لدن المواطنين وحماية حقوقهم؛
- تنمية الوعي القانوني والإداري؛
- جذب الاستثمار وتنشيط الاقتصاد .

دخل قانون الحق في الحصول على المعلومات يوم الثلاثاء 12 مارس 2019، حيز التنقيد بعد سنة من تاريخ نشره بالجريدة الرسمية رقم 6655. وهو بذلك يعتبر أول قانون عرفه بلادنا ينظم كيفية حصول المواطنين المغاربة على المعطيات والوثائق الموجودة في حوزة الإدارات العمومية، والمؤسسات المنتخبة، والهيئات المكلفة بمهام المرفق العام. طبقا للفصل 27 من دستور 2011، وبذلك أصبحت الإدارات العمومية والمنتخبة ملزمة بتقديم المعلومات إلى المواطنين. فبالرجوع إلى مضامين مسودة القانون نجده انه يحتوي على ثلاثين (30) مادة موزعة على سبع (7) أبواب، وفي كل باب حاول من خلاله المشرع شرح وتوضيح كل ما يتعلق بالحق في الحصول على المعلومات (تعريف المعلومة- المعلومات التي يحق للمواطن الحصول عليها-المعلومات التي لا يمكن الحصول عليها-لجنة الحق في الحصول على المعلومات-عقوبات الامتناع عن تقديم المعلومات...) وهذا ما سأحاول ملامسته بالتفصيل.

بالعودة الى مضامين قانون 31.13، نجد أن المشرع قد عرف المعلومات وذلك في المادة الثانية منه واعتبرها المعطيات و الإحصائيات حيث حدد شكلها في (أرقام او حرف او رسوم او صور او تسجيل سمعي او أي شيء أخر) والمضمنة في وثائق ومستندات وتقارير ودارسات ودوريات ومناشير ومذكرات وقواعد البيانات وغيرها من الوثائق ذات الطابع العام. التي تنتجها او تتوصل بها الهيئات المعنية في إطار مهام المرفق العام. كيفما كانت الدعامة الموجودة فيها، ورقية او الكترونية او غيرها. وفي نفس المادة نجد المشرع حدد المؤسسات والهيئات المعنية بهذا الحق (الإدارات العمومية، المحاكم، مجلس النواب، مجلس المستشارين، الجماعات الترابية،

المؤسسات العمومية وكل شخص اعتباري من أشخاص القانون العام، كل هيئة أخرى عامة او خاصة مكلفة بمهام المرفق العام).

طبقا لمواد هذا القانون (قانون 31.13) وبالخصوص المادة الخامسة منه، فالحصول على المعلومات يكون بشكل مجاني، غير أن طالب الحصول على المعلومات يتحمل على نفقته، تكاليف التي يستلزمها عند الاقتضاء (نسخ او معالجة المعلومات المطلوبة وتكلفة إرسالها إليه)، كما منح المشرع الأجانب المقيمين بالمغرب بصفة قانونية حق الحصول على المعلومات وذلك استنادا للمادة الرابعة من القانون نفسه، تطبيقا لأحكام الاتفاقيات الدولية ذات الصلة التي صادقت عليها المملكة المغربية او انضمت إليها.

اما استثناءات من الحق في الحصول على المعلومات، وكما جاء في المادة السابعة فإنه تستثنى من الحق في الحصول على المعلومات، كل المعلومات المتعلقة بالدفاع الوطني وبأمن الدولة الداخلي والخارجي، وتلك المتعلقة بالحياة الخاصة للأفراد او التي تكتسي طابع معطيات شخصية، والمعلومات التي شأن الكشف عنها المس بالحريات والحقوق الأساسية المنصوص عليها في الدستور. ويستثنى ايضا من هذا الحق المعلومات المشمولة بطابع السرية بمقتضى النصوص التشريعية الخاصة الجاري بها العمل من قبيل سرية مداولات المجلس الوزاري ومجلس الحكومة، سرية الأبحاث والتحريات الادارية، سرية المساطر القضائية والمساطر التمهيدية المتعلقة بها، ما لم تأذن بذلك السلطات القضائية المختصة، مبادئ المنافسة الحرة والمشروعة والنزيهة وكذا المبادرة الخاصة، حماية مصادر المعلومات. وهنا ينبغي الإشارة اذا تبين ان جزء من المعلومات المطلوبة يندرج ضمن نطاق الاستثناءات المنصوص عليها في المادة السابعة، يحذف هذا الجزء ويسلم الباقي من المعلومات الى طالبها، هذا ما تطرقت اليه المادة الثامنة من القانون (قانون 31.13) .

اما بخصوص كيفية الحصول على المعلومات، فقد حدد المشرع طرق واجراءات ممارسة هذا الحق وذلك من خلال المادة 14 من القانون ذاته، انه يتم الحصول على المعلومات بناء على طلب يقدمه المعني بالأمر وفق نموذج تعده لجنة اعمال الحق في الحصول على المعلومات، يتضمن الاسم الشخصي والعائلي لصاحب الطلب وعنوانه الشخصي، وعند الاقتضاء، عنوانه الالكتروني، والمعلومات التي يرغب في الحصول عليها، مع ذكر مبررات تقديم الطلب، وبعد ذلك يوجه الطلب الى رئيس المؤسسة او الهيئة المعنية (المؤسسات والهيئات التي حددتها المادة الثانية من القانون) عن طريق الايداع المباشر مقابل وصل او عن طريق البريد العادي او الالكتروني مقابل اشعار بالتوصل. ويجب على الشخص المكلف (المؤسسة او الهيئة المعنية) الرد على طلب الحصول

على المعلومات داخل اجل لا يتعدى (30) يوما ابتداء من تاريخ تسليم الطلب، ويمكن تمديد هذا الآجال لمدة مماثلة اذا لم يتمكن الشخص المكلف من الاستجابة كليا او جزئيا لطلب المعني بالأمر خلال الأجل المذكور، او كان الطلب يتعلق بعدد كبير من المعلومات، واذا تعذر توفير المعلومات خلال الاجل السالف الذكر، او كان تقديمها يحتاج الى استشارة الغير قبل تسليمها، كما يتعين على الشخص المكلف اشعار المعني بالأمر مسبقا بهذا التمديد كتابة او عبر البريد الالكتروني. كل هذا تطرق اليه المشرع من خلال المادة 16 من القانون. اما في الحالات المستعجلة، فيجب على الشخص المكلف الرد على طلب الحصول على المعلومات في اقرب الآجال الممكنة والتي يكون فيها الحصول على المعلومات ضروريا لحماية حياة الاشخاص وسلامتهم، طبقا للمادة 17 من القانون نفسه. هذا بالإضافة الى ان المؤسسات المعنية الزمها المشرع بتعليل ردها كتابيا في حالة رفض تقديم المطلوبة بشكل كلي او جزئي، ويحق لطالب المعلومة عند عدم الرد على طلبه او عدم الاستجابة تقديم شكاية الى رئيس المؤسسة او الهيئة المعنية في ظرف (30) يوما من تاريخ انقضاء الاجل القانوني المخصص للرد على طلبه، او من تاريخ التوصل بالرد، وهنا يتعين على رئيس الهيئة المذكورة دراسة الشكاية واخبار المعني بالأمر بالقرار الذي تم اتخاذه بشأنها خلال خمسة عشر (15) يوما ابتداء من تاريخ التوصل بها، كل هذا تطرق اليه المشرع في المادة 19 من القانون.

من اجل حماية وضمان حسن ممارسة الحق في الحصول على المعلومات، فقد نص المشرع في الباب الخامس من القانون وبالخصوص المادة 22 منه، على لجنة تحدث لدى رئيس الحكومة، وهي لجنة لأعمال الحق في الحصول على المعلومات، والسير على تفعيله، حيث تناط بهذه اللجنة مجموعة من المهام : السير على ضمان حسن ممارسة الحق في الحصول على المعلومات، تقديم الاستشارة والخبرة للهيئات المعنية حول آليات تطبيق احكام هذا القانون وكذا النشر الاستباقي للمعلومات التي بحوزتها، التحسيس بأهمية توفير المعلومات وتسهيل الحصول عليها لاسيما عن طريق تنظيم دورات تكوينية لفائدة اطر الهيئات المعنية...، ويرأس هذه اللجنة رئيس اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، المحدثة بموجب المادة 27 القانون رقم 09.08. وتتألف من ممثلين اثنين عن الادارات العمومية يعينهما رئيس الحكومة وعضو يعينه رئيس مجلس النواب وعضو يعينه رئيس مجلس المستشارين وممثل عن مؤسسة "أرشيف المغرب" وممثل عن المجلس الوطني لحقوق الانسان وممثل عن الوسيط. كما يمكن لرئيس اللجنة ان يدعوا على سبيل الاستشارة، كل شخص او هيئة او ممثل ادارة لحضور اجتماعات اللجنة او الاستعانة

بخبرته. تجتمع اللجنة كلما اقتضت الضرورة ذلك، بدعوة من رئيسها بمبادرة منه او بطلب من نصف أعضائها، ولا تعتبر اجتماعات اللجنة صحيحة إلا بحضور ثلثي اعضائها الحاضرين. كما ان اللجنة تستعين في اداء مهامها بالجهاز الإداري المنصوص عليه في المادتين 40 و41 من القانون رقم 09.08.

نظرا للأهمية البالغة التي يكتسيها هذا القانون في الممارسة الديمقراطية بمشاركة المواطن في الحياة العامة. فإن المشرع نص في المادة 12 من قانون الحق في الحصول على المعلومات على ضرورة تعيين شخصا او اشخاص مكلفين، تعهد اليهم بمهمة تلقي طلبات الحصول على المعلومات ودراستها وتقديم المعلومة المطلوبة، وكذا المساعدة اللازمة، عند الاقتضاء، لطالب المعلومات في أعداد طلبه، فهؤلاء الاشخاص المكلفون بتقديم المعلومات قد يتعرضون للمتابعة التأديبية طبقا للنصوص التشريعية الجاري بها العمل في حالة امتناعهم عن تقديم المعلومات المطلوبة طبقا لأحكام هذا القانون، ويعتبر مرتكبا لجريمة افشاء السر المهني طبقا للفصل 446 من القانون الجنائي، كل من خالف احكام المادة 7 من هذا القانون، وذلك ما لم يوصف الفعل بوصف اشد. وفي نفس المسار نصت المادة 29 من القانون، على ان كل تحريف لمضمون المعلومات المحصل عليها نتج عنه ضرر للهيئة المعنية، او ادى استعمالها او اعادة استعمالها إلى الاساءة او الاضرار بالمصلحة العامة، يعرض الحاصل على المعلومة او مستعملها، حسب الحالة للعقوبات المنصوص عليها في الفصل 360 من القانون الجنائي[1]

الخاتمة

الجريمة المعلوماتية، هي جريمة ذكية، يعمد اليها اشخاص من ذوي المهارات المعلوماتية، لاستغلال معلومات خاصة تخص افراد معينين او شركات او دولا حتى (الهاكار).

هذا النوع الاجرامي هو في تطور مستمر يستغل في ذلك التطور التكنولوجي السريع في مجال المعلوماتي في العالم، ولمجرات هذا النوع الاجرامي الذكي وجب على القوانين ان تكون لينة ومتجددة بحسب ما يجود به عالم التكنولوجيا المتسارع.

[1] - شيماء الهواري: جماعة الضغط الجديدة اللوبي الإعلامي و تأثيره في اتخاذ القرار السياسي نموذج للدراسة: القناتان الفضائيتان الجزيرة القطرية و العالم الإيرانية. أطروحة لنيل دكتوراه الدولة في القانون العام والسياسات العمومية، جامعة الحسن الثاني، كلية العلوم القانونية و الاقتصادية و الاجتماعية، الدار البيضاء، سنة 2017/ 2018

لكن ان نجابه هذا الإجرام بمواد و نصوص قانونية جامدة، ونستغل قوانين مثل الإرهاب او الطوارئ لتصدي له، او اعتباره مطية لتحقيق أهداف سياسية أخرى، هو أمر لن يجر علينا سوى خلق أنواع متطورة من الأصناف الإجرامية الخطير المتطورة .

المغرب يسير نحو المصادقة على مشروع قانون يمنع أي مطالب بمقاطعة او التنديد او تجريح او السخرية او وضع رسم كاريكاتوري يسخر من منتجات اقتصادية استهلاكية او يشكك من قيمتها او جودتها، سواء كانت وطنية او أجنبية تصنع بالمغرب على صفحات مواقع التواصل الاجتماعي، كذلك بخصوص شخصيات سياسية وحزبية وحكومية ايضا، وهو ما يعرف بقانون تكميم الأفواه او مشروع قانون 22.20 .

نفس الأمر نجده في مصر حيث بدأت المطالبة بسرعة إقرار لائحة قانون مكافحة الجرائم الإلكترونية أو جرائم تقنيات المعلومات)، المعروف إعلامياً بـ(مكافحة جرائم الإنترنت)، الذي يهدف إلى تجريم الشائعات والإخبار الكاذبة ضد الحكومة او مؤسسات الدولة المصرية وشخصياتها....

هذا المشروع القانون هو تضييق واضح لحق التعبير والرأي ونشر المعلومات وأيضا حق الحصول عليها، وهو يضرب عرض الحائط كل المكتسبات القانونية السابقة بل يدخل المغرب في مجموعة منتهكي حقوق الإنسان وبالأخص حق الرأي والتعبير والنشر .

التوصيات :

قد يعتبر تقديم أي مقترحات لتعديل او الغاء أي من بنود او مواد قوانين تجريم الجريمة المعلوماتية سواء في مصر او المغرب من المطالب المشرعة اجتماعيا و انسانيا، لكن هنا لن نقوم بمحاولة تخفيف الخناق على أي مجرم انتهك خصوصية أي فرد اخر، لكن ان يتم استغلال مثل هذه القوانين لتصفية حسابات سياسية و ايديولوجية معينة هو امر مرفوض تماما .

لذلك نرجو من المشرع العربي المغربي والمصري ان يكون اكثر شفافية وانفتاحا، والاكثر تقيدا في نفس الوقت بمبادئ القانون العام الدولي والمواثيق الدولي الحامية لحقوق النسان الفردية والجماعية، وألا يستغل النصوص والمواد القانونية المبهمة او التي تقتضي اكثر من تفسير لتطبيق حالة الطوارئ او الاعتقال التعسفي لأسباب ايديولوجية سواء يمينية او يسارية .

لدى نقدم بعض التوصيات التي ارتأينا انها قد تساعد في التقليل من صرامة هذه القوانين وجعلها سيفا ذو حدين لخدمة مأرب سياسية اخرى :

- الغاء الرقابة السياسية على المحتوى السياسي لأي منشور على صفحات المواقع الالكترونية لأنه يدخل ضمن اطار حرية التعبير والرأي وليس أي منشور هو تحريض؛
- قانون الارهاب، في مصر او المغرب، يجب وضع رقابة مشددة في كيفية تطبيقه، وعلى من وجب تطبيقه، والا يعتبر مطية لأغراض سياسية حكومية؛
- القانون المصري والمغربي يركز بشكل كبير على طبيعة الجريمة الالكترونية او المعلوماتية أي الطبيعة المادية (اختلاس اموال) اكثر واغلب المواد تجرمها بشكل قوي، لكن فيما يخص صنف الجريمة الجنسية أي نشر محتويات جنسية للقاصرين او فيديوهات جنسية لأطفال، هو امر قلما تحدث عنه القانونين، مما يجعل أي فعل شائن من هذا النوع يجد ثغرات قانونية او مواد مخففة تناسبه (كما هو الشأن بالنسبة للقانون الجنائي المغرب والعقوبات المخصصة ضد مغتصبي القاصرين والاطفال وذوي الاحتياجات الخاصة فهي غير منصفة).

جرائم ممارسة حرية التعبير في البيئة الرقمية وإثباتها

Crimes of exercising freedom of expression in and in the digital environment

د. درار عبد الهادي
دكتوراه في القانون العام المقارن
جامعة سيدي بلعباس

د. درار نسيمة
أستاذة محاضرة قسم أ
جامعة وهران 02

مقدمة

إن حديث الحرية لسحرا يملك الإنسان على الإنسان لبه ويأخذ بمجامع قلبه فهو حديث الأمس واليوم والغد الذي لا تمل النفس ترديده ولا تسأم الروح من تكراره لأنه الحديث عن القوى المحركة للإنسان.

إن حرية التعبير عن الرأي أصبحت تشكل قوة مؤثرة في الشعوب والأمم خاصة وأن وسائلها تعددت واختلفت من جيل لآخر، ما يعكس جانبها الايجابي في نشر الوعي السياسي والاجتماعي والثقافي أما الوجه أو الجانب السلبي لها هو مساس الغير أثناء ممارسة حرية التعبير في شرفهم وسمعتهم، مما يجعل الفرد يرتكب جريمة السب والقذف في حق هؤلاء. ولم يعد هذا الأمر مقتصر على الجانب التقليدي بل تعداه ليشمل ما هو مستحدث وهو الجانب الرقمي الإلكتروني، وهو أكثر الوسائل المستعملة للتعارف والاتصال بين الناس.

وتكمن أهمية البحث كون موضوع جريمتي السب والقذف مرتبطان بأغلى ما يملك الإنسان وهو حقه في أن يحافظ على شرفه وعرضه واعتباره وأن يصونه من كل ما من شأنه المساس به، والتي ازدادت بفضل الشبكة العنكبوتية وإساءة استخدامها، لذلك تدخل المشرع ووضع النصوص القانونية الواردة حصرا في قانون العقوبات من أجل كبح هاتين الجريمتين وعدم تفاقم وانتشار مثل هذا النوع من الجرائم التي تقع على عرض وشرف الأشخاص.

مما سلف يمكن صياغة الإشكالية التالية: ما مشروعية ممارسة حرية التعبير بالوسائل الإلكترونية الحديثة؟ وهل واكب المشرع الجزائري الجرائم الواقعة من ممارسة حرية التعبير عبر هذه الوسائل الحديثة، خصوصا جريمتي السب والقذف الإلكتروني؟

سوف نقوم بالإجابة على هذه الإشكالية من خلال اعتمادنا على المنهج الوصفي المقارن من خلال تمحيص مواد قانون العقوبات في نصوصه المتعلقة بجريمتي السب والقذف، مما تقتضي علينا الدراسة أن نقسم البحث إلى :

المبحث الأول: تعريف حرية التعبير والوسائل التكنولوجية الحديثة

المبحث الثاني: مشروعية ممارسة حرية التعبير وجرائمها في البيئة الرقمية

المبحث الثالث: إثبات جرائم التعبير بالاستعانة بالذكاء الصناعي.

المبحث الأول: مفهوم مصطلح "حرية التعبير" و"الوسائل التكنولوجية الحديثة"

سوف نقوم في هذا الشق من البحث بتعريف المصطلحات ونتطرق إلى كل من مصطلح حرية التعبير (المطلب الأول) ومصطلح وسائل التكنولوجية الحديثة(المطلب الثاني).

المطلب الأول: تعريف حرية التعبير

عرفت الحرية اصطلاحا بأنها:" المكنة العامة التي قررها الشارع للأفراد على حد السواء، تمكينا لهم من التصرف على خيرة من أمرهم، دون الإضرار بالغير"[1]

وعرفت فقها على أنها "الحق في فعل أي شيء تسمح به القوانين"[2]وكذلك "على أنها حقوق ذاتية متصلة بشخصية الفرد".[3]

وعُرِفَ التعبير لغة هو الإعراب عما في النفس بالكلام أو بالحركات أو بقسمات الوجه.[4]

أما فقها فعرفت حرية التعبير حسب الأستاذ"**L.FAVOREU** " على أنها القدرة على التعبير الحر عن الرأي بشكل شفهي أو مكتوب. بينما يعرفها الأستاذ"**P.WACHSMAN**" على أنها حرية الرأي واستقبال وإيصال الأخبار والآراء بدون تدخل من السلطات العامة وبدون اعتبار للحدود".[5]

---

[1] محمد فتحي الدريني، خصائص التشريع الإسلامي في السياسة والحكم، مؤسسة الرسالة، بيروت، 1982،ص 404.

[2] هذا التعريف مقتبس من جون لوك انظر: كريم كشاكش، الحريات العامة في الأنظمة السياسية المعاصرة، منشأ المعارف، الإسكندرية، 1917، ص 25.

[3] إدموند رباط، الوسيط في القانون الدستوري العام، بيروت، دار العلم للملايين، 1983،ص135.

[4] دايم بلقاسم، حرية التعبير والنظام العام ،، مجلة الحقوق والحريات، جامعة ابو بكر بلقايد- تلمسان-، ع01، 2014، ص20.

[5] محمد هاملي، إشكالية الموازنة بين حرية التعبير واحترام الاديان والرموز الدينية على ضوء احكام القانون الدولي، مجلة الحقوق والحريات، جامعة ابو بكر بلقايد- تلمسان-، ع02،2015،ص11،نقلا عن:

أما على المستوى العربي فعرف نبيل صالح حرية التعبير: "بأنها حق كل إنسان في أن يسوغ آرائه وأفكاره ومعتقداته بحرية علنا وبالطريقة التي يراها مناسبة إن كان ذلك بالكلام أو بكتابة المقالات والكتب أو بتنظيم المظاهرات والمسيرات أو عقد الاجتماعات الشعبية وكل أشكال الاحتجاج إضافة إلى التعبير الحر عن الذات بواسطة الفنون والموسيقى وغيرها من الطرق الأخرى كما تتضمن حق الإنسان في السكوت وعدم الإفصاح عن آرائه إلا بإرادته الحرة."[1]

أما فيصل شنطاوي:" قدرة الفرد على التعبير عن آرائه وأفكاره بحرية تامة بغض النظر عن الوسيلة التي يستخدمها سواءا كان ذلك بالاتصال المباشر بالناس أو بالكتابة، الإذاعة أو الصحف أو بوسيلة الرسالة."[2]

وحرية التعبير تعني حرية الشخص في أن يقول ما يفكر فيه بدون أن يطارد، وتعرف أنها حق الأفراد في التعبير الحر عما يعتقدونه من أفكار دون أن يكون في ذلك مساس بالنظام العام وحقوق الأخرين.[3]

ويمكن تعريف حرية التعبير بأنها حرية الإفصاح عن الأفكار والآراء بطريقتي الكلام أو الكتابة أو عن أي طريق أخر كأن يكون الرسم والتصوير أو أي عمل فني بدون رقابة أو قيود حكومية شريطة أن لا تمس مضامين هذه الأفكار أو الآراء ما يمكن اعتباره خرقا لقوانين وأعراف الدولة ولا تحرض على الكراهية أو العنف أو تدعوا لأفكار شوفينية[4]، وتحترم حريات الآخرين في العبادة والمعتقد ولا تسيء لأي منها.[5]

Patrick WACHSMAN, Libertés publiques, DALLOZ,4^{eme} édition, PARIS, 2002,P 429.

[1] نبيل صالح، حرية التعبير، المؤسسة الفلسطينية لدراسة الديمقراطية (مواطن)، سلسلة مبادئ الديمقراطية، رقم05، 1996،رام الله، ص7 ومايليها

[2] فيصل شنطاوي، حقوق الإنسان والقانون الدولي الإنساني، دار مكتبة الحامد للنشر والتوزيع، ط01، عمان، 1999،ص75.

[3] خاد مصطفى فهمي، حرية الراي والتعبير، دار الفكر الجامعي، الاسكندرية، مصر، 2009، ص 19.

[4] شوفينية أو تزمت وطني: وطنية مفرطة وعدوانية لا تستند إلى منطق معين. وتعني الكلمة أيضا موقفا محتقرا تجاه جنس أو أمة أو ذكر أو أنثى كما هو حال شوفينية الرجال تجاه النساء.

[5] شمخي جبر، الضمانات الدستورية لحرية الرأي والتعبير في الدساتير العراقية، الحوار المتمدن-العدد: 1847 انظر الموقع الإلكتروني: http://www.ahewar.org/debat/show.art.asp?aid=90485 يوم 21-09-2016 على12:53

أما حرية التعبير القضاء الفرنسي، فإن المطلع على قرارات مجلس الدولة الفرنسي هذه الهيئة القضائية وأحكامه يجد أنه يعرف حرية التعبير في قراراته بالاستناد إلى المادة العاشرة (10) من الإتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية. والتي تجعل حرية التعبير تشتمل على العناصر ثلاث وهي: حرية الرأي وحرية الإعلام بالإضافة إلى حق تلقي ونقل المعلومات فجاء في إستنتاجات المقررة العامة لمجلس الدولة الفرنسي السيدة **Fabienne Lambolez** في الفقرة الرابعة من حيثيات القرار "لكل شخص الحق في حرية التعبير ويشمل هذا الحق حرية الرأي وحرية تلقي ونقل المعلومات والأفكار دون تدخل من السلطة العامة ودونما اعتبار للحدود ...."[1]

ونفس المادة من الإتفاقية أُستند إليها في بعض القرارات: كقرار تأييد وزير الثقافة والإتصالات الذي حرم للقاصرين الذين تقل أعمارهم عن **18** عاما من الفيلم السينمائي "الجنين يصطاد في السرية".[2]وكذلك إلغاء قرار اللجنة المشتركة للمنشورات ووكالات الأنباء برفض تجديد شهادة التسجيل الصادرة سابقا للنشر ليون القدم **Lyon Foot** وتحريرها من قبل الشركة العارضة **la société exposante**[3]. وفي قرار رفض إلغاء مرسوم رئيس الجمهورية الفرنسي جاك شيراك **28** يوليو **2006** بحل جماعة **Tribu Ka**[4] بناء على إقتراح وزير الداخلية نيكولا ساركوزي على أساس قانون **10** يناير **1936**.[5]

[1] Décision C.E, N°355815, Lecture du mercredi 6 mars 2013, ….. Considérant qu'aux termes de l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales :"Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière…

[2] Décision C.E، N° 311017 ،Lecture du lundi 6 octobre 2008.

[3] Décision C.E، N° 298828، Lecture du mardi 7 août 2007.

[4] تريبو كا Tribu Ka هي حركة فرنسية تدعي نفسها كمدافع عن "السود"، تم إنشاؤه في عام 2004 من قبل كيمي سابا Kémi Séba وحلها من قبل مجلس الوزراء 26 يوليو 2006.

[5] Décision C.E، N° 296214، Lecture du vendredi 17 novembre 2006.

المطلب الثاني: تعريف وسائل التكنولوجية الحديثة

إن حق إستخدام الشبكة الافتراضية (الأنترنت)[1] من أجل التعبير عن الرأي من المظاهر المتعلقة بالحق في إنشاء الوسائل المناسبة لممارسة حرية التعبير من جهة والحق في تلقي المعلومات من جهة أخرى، ويمثل احد الحقوق اللازمة أو المشتقة من الحق الأصيل المتمثل في حرية التعبير .

أما أشكال التعبير ففصلت في تعريفه المادة 02 من القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما بقولها :" أشكال التعبير : القول أو الكتابة أو الرسم أو الإشارة أو التصوير أو الغناء أو أي شكل آخر من أشكال التعبير، مهما كانت الوسيلة المستعملة"[2]

ولقد أدت التطورات المعاصرة والتقدم العلمي والتكنولوجي، ولاسيما في مجال المعلوماتية الى ظهور وسائل حديثة لإيصال المعلومات ونقلها، ومنها شبكة الأنترنت، لذى فقد أدت هذه الوسيلة إلى إحداث تغييرات ملحوظة في حياة الأفراد، بحيث أصبحت ضرورة لا يمكن الإستغناء عنها في كثير من الأحيان، وأصبح بمقدورهم التعبير عن آرائهم ومعرفة آراء الأخرين بسهولة من خلال هذه الوسيلة، لذا فان هذه الوسائل المعاصرة قد أضيفت الى الوسائل التقليدية للإعلام، على الرغم من كل التغييرات المهمة التي لحقت بالظواهر الإجتماعية من خلال الثورة المطلقة في الإتصال، وعلى كل الأحوال فإن وسيلة الأنترنت تبقى الوسيلة المختلفة والحديثة في نقل المعلومات إحترام الرأي الأخر وعدم مصادرته.

ونرى أن وسيلة الأنترنت زادت مساحة التعبير عن الرأي والرأي الأخر فلقد أصبح مجال تلقى المعلومات والتعبير عنها واسعا جدا وفي فضاء يتسع لآراء جميع الأفراد، وأصبحت هذه الوسيلة هي الأحدث في زماننا الحالي لسهولة وسرعة إستخدامها وأنه بإستطاعة الفرد أن يوصل رأيه إلى أكثر شرائح المجتمع .

ومما لا شك فيه أن مواقع التواصل الإجتماعي في الأنترنت (فيس بوك، تويتر، يوتوب...) غيرت شكل العالم وأصبحت الشعوب تتواصل فيما بينها بشكل أكبر، وهذا ما حدث

---

[1] عرفت الأنترنت على أنها شبكة معلوماتية عالمية تتشكل من مجموعة وطنية و إقليمية وخاصة، موصولة فيما بينها عن طريق بروتوكول الإتصال IP وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها. أنظر، المادة 10 من القانون رقم 18-04 المؤرخ في 10 ماي 2018 المتعلق بتحديد القواعد العامة بالبريد و الإتصالات الإلكترونية.

[2] القانون رقم 20-05 المؤرخ في 28 أفريل 2020، المتعلق بالوقاية من التميز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية 25 لسنة 2020

في الثورات العربية (الربيع العربي) حيث أصبحت نتواصل بشكل أكثر ونتبادل المعلومات والآراء على نحو ما حدث في الثورة التونسية والمصرية واليمنية والسورية في وقتنا الحالي.[1]

المبحث الثاني: مشروعية ممارسة حرية التعبير وجرائمها في البيئة الرقمية

إن الإنسان يملك الحق في التعبير عن رأيه طالما أن ذلك يتم في إطار المشروعية الذي تحددها الدساتير والقوانين، ولكن ممارسة هذه الحرية في المجال المعلوماتي الخصب جعل الناس يعتقدون أنها مجالا مباحا وغير خاضع للقانون، مما فرض تدخل المشرع الجزائري وجعل ضوابط تكبح أو تقف حاجزا أمام ممارسة حرية التعبير في البيئة الرقمية وهو الحق في حماية الأخرين الذين ينبثق عنه الحق في حماية وصيانة الشرف والإعتبار وعدم خدشه، والذي يعد من بين الحقوق المتعلقة بكيان الإنسان وحده، والتي هي في الأصل من المسائل التي لا تقبل المساس أو الخوض فيها. لدى سوف نتطرق إلى مشروعية ممارسة حرية التعبير في الفضاء الرقمي (المطلب الأول)، لجرائم التعبير في البيئة الرقمية (المطلب الثاني)

المطلب الأول: مشروعية ممارسة حرية التعبير في الفضاء الرقمي

إن المتتبع لعالم اليوم يستطيع أن يلاحظ بسهولة الوزن التي أصبحت شبكة الأنترنت تشكله، وخاصة في ظل رياح التغيير التي هبت على الشرق الأوسط وشمال إفريقيا، وتمثل أداة هذا التغيير في شبكة الأنترنت التي تحولت إلى ملتقى كبير يضم كل أطياف المجتمع وطبقاته من طلاب وموظفين ومثقفين وبطالة عن العمل...إلخ، حيث تحولت مواقع التواصل الإجتماعي والمدونات إلى فضاءات لتلاقح الأفكار والتعبير عما يختلج في النفوس، وفي خضم هذا التحول كان للصحف الإلكترونية نصيب في هذا التحول، هذه الأخيرة لا تحتاج لا إلى ترخيص ولا إيداع إخطار لأنها ببساطة عابرة للقارات والحدود..

ومواكبة من المشرع الجزائري للتطور الحاصل في وسائل الإعلام، وبعدما كان قانون الإعلام الملغى رقم 90-07 يهمل تنظيم النشاط الإعلام الإلكتروني ، حرص المشرع الجزائري في القانون العضوي 12-05 المتضمن قانون الإعلام على تنظيم نشاط الإعلام الإلكتروني بشقيه: الصحافة المكتوبة الإلكترونية والإعلام السمعي البصري عبر الأنترنت .

[1] فهد فايز عبد الله العتيبي، الحق في إبداء الراي والتعبير في الدستور الكويتي والمواثيق الدولية(دراسة تطبيقية)، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2012،ص98.

ولقد عرفت الصحافة الإلكترونية طبقا لنص المادة **67** من القانون العضوي **12-05** :" كل خدمة اتصال مكتوب عبر الانترنت موجهة للجمهور أو فئة منه، وينشر بصفة مهنية من قبل شخص طبيعي أو معنوي يخضع للقانون الجزائري، ويتحكم في محتواها الإفتتاحي".

أما الإعلام عبر الأنترنت هي أجهزة الإعلام الالكترونية السمعية البصرية دون غيرها من أجهزة الصحافة الإلكترونية طالما أن نص المادة **66** وردت ضمن الباب المنظم للإعلام السمعي البصري،[1] ولكن بالعودة إلى المادة **03** من قانون الإعلام نجدها تعرف لنا أنشطة الإعلام قانونا على أنها كل نشر أو بث لوقائع أحداث أو رسائل أو آراء أو أفكار أو معارف، عبر أي وسيلة مكتوبة أو مسموعة أو متلفزة أو إلكترونية، وتكون موجهة للجمهور أو لفئة معينة، وهذا التعريف يشمل وسائل الإعلام الإلكترونية السمعية والبصرية والمكتوبة، وما يعزز هذا القول هو أن المشرع نظم كل من الصحافة الإلكترونية والنشاط السمعي البصري عبر الأنترنت ضمن الباب الخامس من قانون الإعلام والموسوم بـ " وسائل الإعلام الإلكترونية ".[2]

بالإضافة إلى ذلك فإن المواد المتعمقة بحضر الصحف الأجنبية في بعض القوانين المنظمة لإصدار الصحف في الدول العربية ذات أثر محدود وذلك بوصف أن المبحر عبر الأنترنت يمكنه الولوج إلى أي صحيفة في العالم، وحتى بعض الحلول التقنية التي تلجأ إليها بعض الدول لممارسة الرقابة على الأنترنت والمتمثلة في حجب بعض المواقع لا يمكن أن تستمر للأبد، حيث أن التجارب أظهرت أن البلدان التي تتخذ من العزلة منهجا وذلك لقطع الصلات مع العالم الخارجي خوفا من تأثيراته المحتملة سرعان ما تعرضت لهزات عنيفة جدا ناتجة عن الكبت الممارس ضد المواطنين،

---

[1] نعتقد ان المشرع الجزائري يكون قد وقع في خطا منهجي وجانبه الصواب حينما ادرج شروط تأسيس وسائل الإعلام الإلكترونية ضمن الباب الرابع الخاص بخدمة الإعلام السمعي البصري وكان عليه ان يدرجها في الباب الخامس الخاص بوسائل الغلام الإلكترونية درءا لكل لبس، مع العلم ان مشروع القانون العضوي المتعلق بالإعلام كان يدرج المادة التي تشترط خضوع الإعلام الإلكتروني بنوعيه (السمعي البصري والمكتوب) الى اجراء التصريح المسبق ضمن الباب الخامس الخاص بوسائل الإعلام الإلكترونية. أنظر المادة70 من مشروع القانون العضوي المتعلق بالإعلام .

[2] محمد هاملي، ضوابط ممارسة حرية الإعلام عبر الانترنت في القانون الجزائري، مجلة الحقوق والحريات، جامعة أبو بكر بلقايد- تلمسان-، العدد03،2016،ص242 ومايليها -بتصرف-

حيث أنه كلما كان القمع أكبر كانت درجة الإنفجار بقدره، وما النموذج التونسي، وبعده المصري ثم الليبي إلا خير دليل على ذلك.[1]

المطلب الثاني: جرائم التعبير في البيئة الرقمية

تحت عنوان حماية شرف وإعتبار الأشخاص وحياتهم الخاصة إهتمت الإتفاقيات الدولية والتشريعات الداخلية بحماية الحياة الخاصة وحظرت الإعتداء عليها ومن قبيل ذلك ما نصت عليه المادة 12 من الإعلان العالمي لحقوق الإنسان التي منعت التدخل في حياة الفرد الخاصة وأسرته ومسكنه ومراسلاته، ومنعت الإعتداء على شرفه وسمعته من خلال تكريس حماية قانونية ضد هذا التدخل، ونفس الإتجاه سار عليه العهد الدولي الخاص بالحقوق المدنية والسياسية التي منحت حماية قانونية للفرد من أي تدخل أو إعتداء على خصوصياته أو عائلته أو مراسلاته أو شرفه وسمعته.

يتعين إذن على كل دولة أن تضع قوانين تحمي بها مواطنيها من أي إعتداء على حياتهم الخاصة أو سمعتهم، وقد وضع المشرع الجزائري نصوصا تجريمية وعقابية لمواجهة الأفعال الماسة بشرف وإعتبار الأشخاص وحياتهم الخاصة وهي تشمل جرائم القذف والسب والوشاية الكاذبة[2] والإعتداء على الحياة الخاصة وستقتصر دراستنا على جريمتي السب والقذف بطابعها الرقمي وما جاء من نصوص لمجابهتها.

بداية لابد من الإعتراف أن المشرع الجزائري بدأ يوكب التطورات التكنولوجيا المستحدثة في عدة مجالات كالتوثيق الإلكتروني وعصرنة قطاع العدالة والتجارة الإلكترونية...إلخ[3]، إلا أنه لا يوجد قانون خاص ينظم الجرائم المعلوماتية المتعلقة بجريمة السب والقذف عن طريق الأنترنت، وإنما يتم العقاب على هاتين الجريمتين بموجب أحكام مواد قانون العقوبات، حيث يعتبر الإنترنت من الوسائل المنصوص على إستخدامها من أجل ممارسة حرية التعبير وقد سبق بيان مشروعيتها. لذلك سوف نقوم بتفصيل الجريمتين كل على حدى كالتالي:

أولا:جريمة القذف

---

[1] سالمي عبدالسلام، حرية إصدار الصحف في الدول العربية بين نظامي الترخيص والإخطار وواقع التطور التكنولوجي، مجلة جامعة تكريت للعلوم القانونية والسياسية، ع10، المجلد03، العراق،2011، ص 81.

[2] وتشترك جريمتي القذف والسب والوشاية الكاذبة في كونها ترد على شرف الأشخاص وإعتبارهم، ويقصد بالشرف الكيان الأدبي للفرد أي شعوره وكرامته وإحساسه والمكانة التي يتبوأها في المجتمع.

[3] القانون رقم 15-04 المتعلق بالتوثيق الإلكتروني، القانون رقم 15-03 المتعلق بعصرنة قطاع العدالة، القانون رثم 18-05 المتعلق بالتجارة الإلكترونية......إلخ

وتعرف على إسناد واقعة محددة تستوجب عقاب من نسب إليه أو إحتقاره إسنادا علنيا معديا[1].

وعرفتها المادة **296** من قانون العقوبات "يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف أو إعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الإسم ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة. "

تحقق جريمة القذف طبقا لنص المادة **296**[2] من قانون العقوبات عند الإدعاء بواقعة وإسنادها لشخص معين، بحيث تمثل إعتداء على شرفه أو إعتباره المعنوي على أن يتم ذلك بشكل علني بأي وسيلة من وسائل التعبير كالقول أو الكتابة في الجرائد والمجلات أو أجهزة الإعلام السمعية البصرية أو وسائل الإتصال الإلكترونية، يستوي في ذلك أن يتم القذف عن طريق الصحافة والإعلام أو بغير ذلك من الوسائل.

وهذا ما يمكن أن يقع بواسطة شبكة الأنترنت من بث رسائل تحقير لشخص معين أو لطائفة معينة وأن فعل العلانية يشمل جميع الوسائل التقليدية والإلكترونية والوسائل التكنولوجية التي قد تستحدث مستقبلا وكل ما من شأنه أن يؤدي إلى الإفصاح عن هذا التعبير أو الرأي، فيمكن أن يقع بواسطة شبكة الأنترنت سواء بإرسال رسالة إلى جميع المشتركين في الشبكة، فبمجرد فتح الجهاز نجد الرسالة ونطلع عليها أو بأي وسيلة أخرى تؤدي إلى النتيجة التي أرادها الجاني من فعله، ويتضح لنا هنا أن جريمة القذف تقوم على فعلين أولهما هو الإفصاح عن الجريمة وثانيها هو حالة التعبير عن الواقعة بإداعتها عبر شبكة الأنترنت التي تعطيها صفة العلانية التي تفترضها الجريمة وفي الغالب يرتكب الفعل شخص واحد ولكن إذا إرتكب الفعلين من شخصين

---

[1] الأمر رقم 66 – 156 مؤرخ في 18 صفر عام 1386 8 يونيو 1966 المتضمن قانون العقوبات .

[2] المادة 296:" يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذآر الاسم ولكن كان من الممكن تحديدهـما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة." عدلت بالقانون رقم 06-23 المؤرخ في 20ديسمبر2006الجريدة الرسمية رقم84

مختلفين فكلاهما فاعل أصلي للجريمة، ويعني ذلك أن من إقتصر نشاطه على مجرد أعطاء العلانية لواقعة ذكرها غيره يعد معه فاعلا للقذف.

وبالرجوع إلى هذه المادة نستنتج بأنها تتكون من ثلاثة أركان وهي:

1. **الركن الأول: فعل الإدعاء أو الإسناد:**

فالإدعاء يحمل معنى الرواية عن الغير أو ذكر الخبر محتملا الصدق والكذب

أما الإسناد يفيد نسبة الأمور إلى شخص المقذوف على سبيل التأكيد سواء كانت الوقائع المدعي بها صحيحة أو كاذبة[1].

ويتحقق القذف على فعل الإسناد الذي ينصب على واقعة محدودة من شأنها عقاب المجني عليه أو إحتقاره، ولا يشترط هنا أن يثبت القاذف صحة ما قذف به حتى تطبق عليها العقوبة في حالة عجزه أو إمتناعه عن ذلك.[2]

لذا فعلى كل صحفي أو مؤلف لمقال أو المعلق بصفة عامة ؛ عند ممارسته لحقه في الإعلام أو حرية التعبير عن رأيه سواء عن الطريقة التقليدية أو الطبيعة الرقمية على مستوى الأنترنت أن يدرك طبيعة ما ينشره أو يذيعه أو يبثه من أقوال يسند فيها وقائع يكون موضوع لجريمة القذف

---

[1] أحسن بوسقيعة الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة 04، دار هومة، الجزائر، 2006، ص 190

[2] هنالك فرق بين القذف والنقد الذي يكون أيضا علنيا. النقد لا يوجه لذاته الشخص بل لما يشغل من منصب وما يؤدي من مهام، وحتى نبتعد عن دائرة التجريم، والبقـاء في دائرة حرية الرأي والتعبير لا بدمن توافر شروط معينة ممكن أن نجملها بم ايلي:

1. يكون الأمر الذي أنتقد فعلا حقيقيا وواقعيا.
2. أن يكون وصف الواقعة أو العمل الذي قام به الشخص ملائما لحال الواقعة دون مبالغة فيه.
3. أن تكون الواقعة اجتماعية لها أهمية عند أفراد المجتمع، وليس أمرا شخصيا يتعلق بحال الشخص المنتقد.
4. وأن تكون حسن النية عند الشخص الناقد الذي يعبر عن رأيه فلا يكون سيء النية وهدفه من نشر الواقعة والحديث عنها والترويج ضدها هو التشهير بمن قام بها، بل يجب أن يكون هدفه هو نشر الحقيقة واطلاع العامة عليها. أنظر: صويص سليمان، حرية الرأي والتعبير في المواثيق الدولية، مجلة الرسالة، مجلة عن المركز الوطني لحقوق الإنسان، العدد 11. ص28وما يليها. وأيضا أنظر: كامل السعيد، حق النقض في كل من الدستور وقانون المطبوعات والنشر، مجلة الرسالة، المركز الوطني لحقوق الإنسان، ص 2و3.

المعاقب عليها في القانون ؛ بحيث يكون بذلك قد تعسف في إستعمال حقه في ممارسة حرية التعبير[1].

الركن الثاني: العلنية : وهو الركن المميز لجنحة القذف فإن غاب هذا الركن أصبحت الجريمة مجرد مخالفة يعاقب عليها القانون في المادة **3/463** بعنوان السب غير علني[2] ، والغرض من العلنية هو التشهير بالمجني عليه، مما يؤدي إلى المساس بسمعته واعتباره عن طريق الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات ...

2. **الركن الثالث :القصد الجنائي :** هو معرفة وإدراك الجاني من أن فعله أو إنصراف إرادته إلى أن فعله أو تعبيره العلني يشكل خدشا ومساسا لشرف وإعتبار المقذوف ؛ ولا يستلزم القانون نية الإضرار فالقصد العام يكفي وحده لقيام الجريمة دون القصد الخاص.

أما العقوبة على الجريمة نصت عليها المادة **298** من قانون العقوبات وهي الحبس من شهرين إلى ستة أشهر وبغرامة من **25000** إلى **50000** دج أو بإحدى هاتين العقوبتين ؛ ويعاقب على القذف الموجه إلى الشخص أو أكثر بسبب إنتمائهم إلى مجموعة عرقية أو مذهبية أو إلى دين معين بالحبس من شهر إلى سنة وبغرامة من **10.000** إلى **100.000** دج إذا كان الغرض هو التحريض على الكراهية بين المواطنين أو السكان.

والملاحظ أن القانون الجزائري لا يعتد بحسن النية ؛ وهذا خلافا لما هو عليه القانون الفرنسي.

ثانيا: جريمة السب : تعرف طبقا لنص المادة 297 من قانون العقوبات " يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة " ويقصد بالسب كل خدش للشرف والإعتبار، فهو مدلول أوسع من القذف الذي لا يتحقق إلا بإسناد واقعة معينة.

ونستطيع القول أن بإنطباع نص السب بواسطة الهاتف على الجرائم الواقعة عن طريق الأنترنت على إعتبار أن الأنترنت يعتمد في أساسه على الإتصال الهاتفي، كما أنه ليست جميع

---

[1] زمورة داود، الحق في الإعلام وقرينة البراءة، رسالة ماجيستر، كلية الحقوق - بن عكنون الجزائر،2006، ص70.

[2] زمورة داود ،المرجع السابق، ص195

الجرائم التي تقع غير علانية، وذلك بعد ظهور الهواتف الجماعية والمرئية وغيرها التي توفر العلانية التي يتطلبها المشرع في مواد السب. كالإتصال في مجموعات المسنجر والوات ساب والتويتر..إلخ.

من خلال التعريف يمكن استنتاج الأركان التالية :

1. **الركن الأول :** التعبير المشين أو البذيء : وذلك دون إسناد واقعة معينة للشخص عكس القذف وتكون هذه العبارات تحتوي على كلام ماجن ؛ كالزاني ؛ السكير ؛ المجرم ...
2. **الركن الثاني** : العلانية : وتحقق هذه العلانية بالكتابة أو القول أو الصور أو الوسائل السمعية والبصرية، وهنا تشمل جميع الوسائل بما فيها الوسائل الرقمية الحديثة أو ما قد يستجد في هذا المجال مستقبلا .
3. **الركن الثالث : القصد الجنائي :** وهو إنصراف إرادة الجاني وعلمه بالجهر بالألفاظ المشينة

أما العقوبة : لقد أورد المشرع الجزائري مجموعة من النصوص تعاقب على كل من السب الموجه لرئيس الجمهورية؛ وللرسول الله صلى الله عليه وسلم وبقية الأنبياء طبقا لنص المواد **144** مكرر **1** و**144** مكرر **2**.

ومن أهم التطبيقات العملية للعقوبة على جريمة السب الحكم الصادر في **25** يناير **2005** عن محكمة سيدي محمد الجزائر العاصمة الذي قضى بإدانة مدير يومية الخبر ومدير يومية الوطن بـ **06** أشهر حبسا موقف النفاذ وغرامة قدرها **50000** دج في حق كل منهما بالإضافة إلى غرامة في حق كل من الصحيفتين مقدارها **03** ملايين دج[1].

المبحث الثالث: إثبات جرائم التعبير في البيئة الرقمية إستعانة بالذكاء الصناعي.

لقد أثبتت تقنيات الكمبيوتر نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها كما يمكن الاستعانة بالذكاء الصناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم إستنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالكمبيوتر وفق برامج صممت خصيصا لهذا الغرض.[2]

---

[1] هاملي محمد، التجربة الجزائرية في حرية الإعلام، رسالة ماجيستر، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2005، ص 113

[2] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية -دراسة مقارنة-، ط01، دار الفكر الجامعي، الإسكندرية -مصر، 2018، ص308.

وفي إطار جرائم الأنترنت فإنه يميز بين الأدلة التي يلزم التحفظ عليها داخل جهاز الحاسب الألي وبين تلك التي يلزم بقاءها في العالم الإفتراضي، وبين أيضا تلك النوعية من الأدلة التي تنتمي إلى العالم الرقمي، ومع ذلك يمكن اللجوء إلى إخراجها من إطار الحاسوب والعالم الرقمي إلى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة تساعد في الإدانة، وكذلك في البراءة [1].

إن التحفظ على الأدلة داخل جهاز الكمبيوتر من العمليات المعقدة التي تحتاج بداية إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر، وهذا الأمر يستلزم بالضرورة حركة الكمبيوتر سيما من حيث الخلل والعطب، ويعطي العدوان الفيروسي مقالا حيويا هنا، إذ يكفي أن يكون هناك فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستفادة هذا الكمبيوتر، مثل هذا الإتجاه نجده في التشريع الإنجليزي.

وتتم عملية حفظ الأدلة داخل جهاز الكمبيوتر بأساليب متعددة تمثل في أبسط مظاهرها باستخدام اسلوب الحفظ العادي وأقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه ذلك، إن الدليل الرقمي هو في العادة ملف يحتوي على بيانات رقمية تعطى مظهرا معلوماتيا محددا غير قابل للتحويل إي مظهر أخر إلا بإجراء تعديلات رقمية في البيانات المذكورة.

أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي، فإنه يتطلب من الخبير التقني القيام برصد موقع الأنترنت أو المعلومات التي تشير إلى الجريمة والتي تكون في مظاهر مختلفة الأشكال، كما لو كانت الجريمة من جرائم القذف والسب في غرف المناقشة، ففي مثل هذه الحالة الأخيرة يتم اللجوء إلى الخادم الذي تولى ربط هذه الغرف عبر العالم الرقمي، ولكي يمكن التوصل إلى تحديد موضوع السب والقذف وتاريخه وإذا كانت الجريمة من جرائم النشر عبر الأنترنت فقد يكتفي بمجرد اللجوء إلى ذاكرة الحاسب الألي المستخدم هنا دون وحاجة إلى تحديد الخادم ... إلخ

ففي مثل هذه الحالات يقوم الخبير باستخدام برمجيات مساعدة للتوصل إلى القيم بالحفظ في العالم الرقمي، كما هو الشأن في حجز وتشفير مثل هذه المواقع بعد تحديد جدليتها ودقتها ومسارها، هذا أمر يترتب عليه عدم إمكانية حذفها من العالم الرقمي، وإذا قام أحدهم بذلك فإن ذلك يعد قرينة على أنه هو من إرتكب الجريمة.

---

[1] خالد ممدوح ابراهيم، حجية البريد الإلكتروني في الإثبات، ط01، دار الفكر الجامعي، الإسكندرية –مصر، 2018، ص 201.

وتستدعي عملية حفظ الأدلة في العالم الإفتراضي لزوم قيام الخبير بعرض الأدلة في المحكمة أو على جهات التحقيق، ومثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة كما هو الشأن حال عرض الدليل المقدم إلى المحكمة الموضوع أمام جهة قضائية أعلى كالإستئناف أو الطعن بالنقض.

ودرءا للمشكلات التي يمكن أن تنجم عن حفظ الأدلة في العالم الرقمي فإن العديد من المحاكم لجأت إدارتها رقميا، بحيث يتم تسليم الأدلة إلى إدارة متخصصة تتولى بدورها حفظ الأدلة في العالم الرقمي لعرضها على القضاء كلما تطلب الأمر ذلك [1].

فلقد سهلت وسائل الإتصال التكنولوجية عملية ادراك الجرائم والتحكم فيها عن بعد نظرا لتوفر تقنيات حديثة مثل الهاتف النقال، الأنترنيت والحاسبات المتطورة [2].

وإدراكا منه لهذا التهديد، فان الدرك الوطني قد اعتمد في نشاطه المرتقب الرامي إلى مواكبة إنتقال المجتمع الجزائري نحو العصر الرقمي، في السنوات الأخيرة، استراتيجية وطنية تهدف إلى مواجهة أثار الثورة التي تنقلها تكنولوجيا المعلوماتية والاتصالات الجديدة [3].

وفي الختام لا بد من التنويه على أنه يجب أن يكون قاضي موضوع الوقائع الجزائية التي تتصل بالأنظمة الرقمية، على دراية بالقدر اللازم من المعلومات المتصلة بقيامه بفحص سلامة المنهج المستخدم والأدوات المتصلة بفحص الأدلة الرقمية، فينبغي عليه :

- أخذ في الحسبان أن الجرائم المعلوماتية لا تترك أي أثر بعد ارتكابها لأنها تعتمد على الخداع في إرتكابها والتضليل في التعرف على مرتكبيها [4]
- القيام بعملية النسخ باستخدام الأدوات المناسبة.
- التأكد من اجراءات التثبت من عدم القيام بالتلاعب بالمحتوى الرقمي وعدم التعديل به أثناء اجراءات استخلاصه.
- استخدام أدوات ومنهج سليم في مرحلتي المعالجة وتحليل الأنظمة الرقمية، وفقا لمعايير القوانين المعتمدة في هذا الشأن.

---

[1] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية -دراسة مقارنة-، المرجع السابق، ص310.

[2] بدراوي قويدر، التكنولوجية والجريمة المستحدثة، مجلة الدركي، ع 14، خلية الاتصال بقيادة الدرك الوطني، الجزائر أكتوبر 2007، ص23.

[3] راجع تفصيل ذلك، خالد ممدوح ابراهيم، حجية البريد الإلكتروني في الإثبات، المرجع السابق، ص42.

[4] عبلة سليم، المساس بأنظمة المعالجة الالية للمعطيات، مجلة المستقبل، ع 29، مدرسة الشرطة طيبي العربي بسيدي بلعباس، الجزائر أفريل 2008 ص 15.

- كتابة تقرير يحتوى على كافة التفصيلات التي تمت لإستخراج الدليل الرقمي.
- القيام بعرض الدليل الرقمي بالصورة التي توضح كل ما تم بشكل مبسط لقاضي الموضوع.

وبذلك يتمكن القاضي من الوصول إلى اليقين في الدليل الرقمي، مما يمكن القاضي من الحكم إما بالبراءة أو الإدانة في الواقعة المنظورة أمامة، ولا شك أن الأمر يلقى بعبء كبير على سلطات الإستدلال والتحقيق، وكذلك المختصين الفنيين بالعمل الجنائي للحاسب لاتباع المنهج السليم في إستخلاص الدليل وتتبع أحدث المستجدات في تقنيات علوم الحاسب الجنائي للوصول إلى أفضل النتائج ودقتها [1].

الخاتمة

لقد تعددت منابر حرية التعبير لكي تكون مسارح لعرض ثقافات مختلفة وليست مسرحا للتجاوزات عن طريق السب والقذف التي تنصب على شرف وإعتبار الأفراد، منها ما يشترط العلانية كشرط أساسي لقيامها كجريمتي القذف والسب العلني، ومنها ما لا يشترط العلانية كجريمة السب غير العلني التي يمكن إقترافها بوسائل تكنولوجية جد متطورة. بإعتبار أن المشرع تطرق لمثل هذه الجرائم بطابعها التقليدي في قانون العقوبات وجعل من العالم الإفتراضي وسيلة لها فقط،

و كما هو معلوم بأن الجرائم الواقعة في مواقع التواصل الإجتماعي قد تعددت أثارها بفضل الوسيلة الإلكترونية المستعملة، الأمر الذي يؤدي بنا إلى صعوبات جمة في تحقيقها وإثباتها نظرا لسهولة إتلاف أدلتها من قبل الجناة الفاعلين لها. وأيضا بتخطيها كافة الحدود الجغرافية ليس للدول فقط وإنها للقارات بسهولة ويسر.

وتطوى أوراقنا البحثية بالتوصيات التالية:

1. لابد على المشرع الجزائري أن يقتدي بالتشريعات المقارنة التي جرمت وعاقبت على الأفعال الواقعة في العالم الرقمي مع التركيز على تلك التي تتستر وراء ممارسة حرية التعبير.

[1] خالد حازم ابراهيم، دور الاجهزة الامنية في الاثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية الانترنت "دراسة مقارنة"، الطبعة 01، دار النهضة العربية للنشر والتوزيع، مصر، 2014، ص ص 181، 182.باعزيز أحمد، الخبرة ودورها في الإثبات الجنائي، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2018-2019،ص495

2.وضرورة وضع ترسانة إجرائية لمتابعة مثل هذا النوع من الإجرام السبراني الذي ينصب على أعراض وشرف الأفراد، كالتفتيش الرقمي وحفظ الأدلة الإلكترونية والفصل في مسألة تنازع الإختصاص القضائي.

3.لابد من وجود تعاون أمني وقضائي بين مختلف الجهات الوطنية والدولية من اجل تكوين قضاة ولرجال متخصصين لمجابهة مثل هاته الخروقات، وأيضا ضرورة إلزام أصحاب مواقع التواصل الإجتماعي بوضع الهوية الحقيقية للإسراع في إجراءات التعرف عليهم وتحديد مكانهم



Berlin10315 Gensingerstr :112
Tel :0049-code Germany
54884375-030
91499898-030
86450098-030
book@democratica.de